APOGEE *Communications*

Rapport de
Veille Technologique Sécurité
N°53

Décembre 2002

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: mailing-lists, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Les symboles d'avertissement suivants seront éventuellement utilisés:

- Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire de faire encourir un risque sur le système d'information associé.
- Site susceptible d'héberger des informations ou des programmes dont l'utilisation est répréhensible au titre de la Loi Française.

Aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur **WEB**.

La diffusion de ce document est restreinte aux clients des services VTS-RAPPORT et VTS_ENTREPRISE

Les marques et les produits cités dans ce rapport sont la propriété des dépositaires respectifs.

APOGEE Communications
1, Rue Jean Rostand
91893 ORSAY CEDEX

Pour tous renseignements
Offre de veille: http://www.apogee-com.fr/veille
Informations: vts-info@apogee-com.fr

© APOGEE Communications - Tous droits réservés

Au sommaire de ce rapport …

PRODUITS ET TECHNOLOGIES 5
LES PRODUITS 5
INTRUSION 5
PSIONIC - CLEAR-RESPONSE 5
FWLOGWATCH V0.9 5
LES TECHNOLOGIES 7
JAVA 7
LSDPL - JAVA ET LA SÉCURITÉ 7
ASP.NET 8
MICROSOFT – BUILDING SECURE ASP.NET APPLICATION 8
INFORMATIONS ET LÉGISLATION 10
LES INFORMATIONS 10
INCIDENTS 10
CSIRT – LES SERVICES 10
CERT – TRACER LES ATTAQUES 11
CRYPTOGRAPHIE 12
ECCP-109 – DÉFI REMPORTÉ 12
SÉCURISATION 13
NSA - GUIDE TO SECURING MICROSOFT INTERNET EXPLORER 5.5 USING GROUP POLICY 13
NSA - GUIDE TO SECURING MICROSOFT WINDOWS XP 15
NSA - CATALOGUE DES GUIDES DE SÉCURITÉ 16
LA LÉGISLATION 17
USA 17
DECSS – LA COMPÉTENCE DES TRIBUNAUX CALIFORNIENS REJETÉE 17
LOGICIELS LIBRES 19
LES SERVICES DE BASE 19
LES OUTILS 19
NORMES ET STANDARDS 21
LES PUBLICATIONS DE L'IETF 21
LES RFC 21
LES DRAFTS 21
NOS COMMENTAIRES 26
LES RFC 26
RFC3436 26
LES DRAFTS 26
DRAFT-IETF-INCH-IODEF-00 26
DRAFT-IETF-INCH-IODEF-RFC3067BIS-REQUIREMENTS-00 28
ALERTES ET ATTAQUES 30
ALERTES 30
GUIDE DE LECTURE 30
FORMAT DE LA PRÉSENTATION 31
SYNTHÈSE MENSUELLE 31
ALERTES DÉTAILLÉES 32
AVIS OFFICIELS 32
BEA 32
CISCO 32
HP 32
HP/COMPAQ 33
IBM 33
LINUX CALDERA 33
LINUX DEBIAN 33
LINUX REDHAT 33
LINUX SUSE 33
MACROMEDIA 34
MICROSOFT 34
NETSCREEN 34
SCO 35

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

SGI 35
SSH 35
SUN 35
TREND MICRO 36
WGET 36
ALERTES NON CONFIRMÉES 36
APACHE 36
FETCHMAIL 36
LINKSYS 36
MACROMEDIA 36
MYPHPLINKS 37
MYSQL 37
SYBASE 37
SYMANTEC 37
TRACEROUTE NG 37
TRENDMICRO 37
WINAMP 37
AUTRES INFORMATIONS 37
REPRISES D'AVIS ET CORRECTIFS 37
CIAC 37
FREEBSD 38
HP 38
IBM 39
LINUX CALDERA 39
LINUX DEBIAN 39
LINUX MANDRAKE 39
LINUX REDHAT 40
SGI 40
SUN 40
CODES D'EXPLOITATION 40
ORACLE 40
BULLETINS ET NOTES 40
CERT 40
VIRUS 41
ATTAQUES 42
OUTILS 42
PAKETTO KEIRETSU 42
TECHNIQUES 46
WINDOWS PROTECTED STORAGE 46
OPENSSL / SLAPPER 6 MOIS APRÉS 48

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Le mot de la rédaction …

Ce mois de décembre verra le 25 Décembre après-midi la publication du numéro 60 du célèbre magazine '**PHRACK**'. La qualité technique des articles publiés par ce magazine nous amène à penser que ceux-ci – sans les avoir encore lus - nous fourniront une excellente matière première pour notre premier rapport de l'année 2003.

Pour finir ce rapide éditorial, nous conseillons la lecture de l'excellente note d'information publiée fin novembre par le **CERTA** sous le titre de '**Chronique d'un incident ordinaire**', titre bien plus évocateur que la référence **CERTA-2002-INF-003** …

❄ ❄ ❄ ❄

🕯 Nous terminerons notre propos en souhaitant à tous nos lecteurs de 🕯 🕯 joyeuses fêtes de Noël et, avec un peu d'avance, une bonne Année 2003. 🕯

★ ★ ★ ★

L'équipe de Veille Technologique

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

PRODUITS ET TECHNOLOGIES

LES PRODUITS

INTRUSION

PSIONIC - CLEAR-RESPONSE

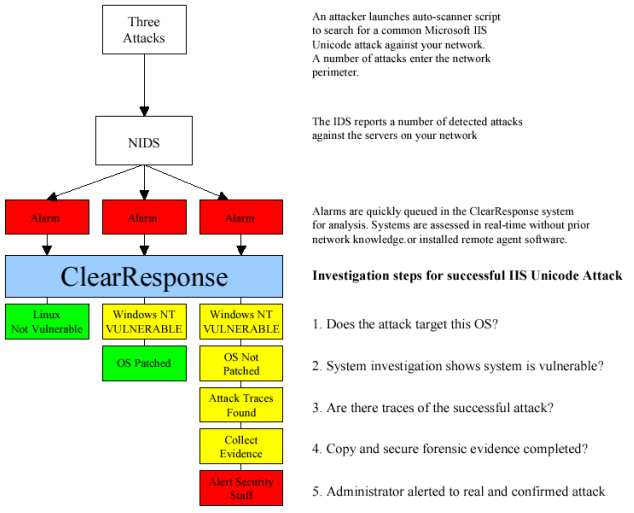
▪**Description**

Connue pour ses produits de surveillance '**LogSentry**', '**PortSentry**' et '**HostSentry**' désormais regroupés dans le paquetage '**TriSentry**', la société '**PSIONIC**' dispose d'une technologie innovante permettant d'assurer la levée de doute à la suite d'une détection d'intrusion.

Annoncée en Juin 2002, la technologie '**ClearResponse**' intervient comme complément d'un système de détection d'intrusion existant en analysant en temps quasi-réel la fiabilité et l'impact des évènements que celui-ci remonte. A ce jour, aucune documentation détaillée n'est hélas disponible hormis un 'white paper' de 6 pages présentant les grands principes du procédé sans aborder cependant aucun élément concret permettant de quantifier l'impact et les performances en environnement de production.

L'idée fondamentale est de réduire le temps de latence existant entre la détection d'une attaque potentielle par un **IDS** et la validation de la réalité et de l'efficacité de celle-ci sur l'ensemble des cibles visées. Pour cela, **ClearResponse** engage automatiquement la démarche d'analyse suivante dès la détection d'un incident:

1- Validation de la vulnérabilité des plates-formes cibles de l'attaque par étude du système d'exploitation de celles-ci.
2- Contrôle du niveau de mise à jour des plates-formes pour lesquelles le système d'exploitation a été confirmé vulnérable à l'attaque.
3- Analyse détaillée des cibles effectives de l'attaque en se basant sur les spécificités de celle-ci. Cette analyse est effectuée au moyen d'un accès privilégié en lecture seule (sic).
4- Dans la cas d'une compromission confirmée, archivage des éléments de preuve pour analyse ultérieure en un lieu sûr (sic).
5- Confirmation de la notification d'attaque et de sa nature auprès des administrateurs désignés.


Three Attacks
An attacker launches auto-scanner script to search for a common Microsoft IIS Unicode attack against your network. A number of attacks enter the network perimeter.
NIDS
The IDS reports a number of detected attacks against the servers on your network
Alarm
Alarm
Alarm
Alarms are quickly queued in the ClearResponse system for analysis. Systems are assessed in real-time without prior network knowledge or installed remote agent software.
ClearResponse
Investigation steps for successful IIS Unicode Attack
Linux Not Vulnerable
Windows NT VULNERABLE
Windows NT VULNERABLE
1. Does the attack target this OS?
OS Patched
OS Not Patched
2. System investigation shows system is vulnerable?
Attack Traces Found
3. Are there traces of the successful attack?
Collect Evidence
4. Copy and secure forensic evidence completed?
Alert Security Staff
5. Administrator alerted to real and confirmed attack
Total elapsed time: Five seconds

Dessin extrait de la brochure PSIONIC

Si les principes exposés nous semblent parfaitement viables et similaires en tout point aux démarches habituellement engagées lors d'une présomption de compromission, plusieurs inconnues demeurent vis à vis des contraintes et des mécanismes de collecte ou de validation. La présentation technique du produit indique en introduction (précepte N°3 'no Remote Agent') que celui-ci ne nécessite aucunement l'installation d'agents spécialisés sur chacun des systèmes mais omet malencontreusement de préciser la nature du canal d'accès 'privilégié en lecture seule'.

L'annonce en octobre dernier par la société **CISCO** de sa volonté d'acquérir la société **PSIONIC**, opération devant être finalisée mi-2003, laisse entendre que les spécifications de ce produit pourraient fort bien évoluer dans les mois à venir. On notera que cette acquisition ramènera dans le giron de la société **CISCO** quelques un des développeurs (dont Craig Roland, le fondateur de **Psionic**) ayant quitté la société '**WheelGroup**' spécialisé dans les systèmes d'**IDS** lors de son rachat par **CISCO** en 1998 …

▪**Complément d'information**

http://www.psionic.com/products/clearresponse.html
http://www.esecurityplanet.com/prodser/article/0,,10753_1368331,00.html

FWLOGWATCH V0.9

▪**Description**

Développé par Boris Wesslowski du '**RUS-CERT**' (Université de Stuttgart), '**FwLogWatch**' facilite la présentation des événements journalisés par les dispositifs de sécurité les plus connus dont **Snort, Cisco PIX** et **IOS**, **NetScreen**, Windows XP, Linux **IPChains**, **NetFilter** et **Iptables**, Solaris/BSD/Irix/HP **ipfilter** …

Les formats de journalisation supportés sont automatiquement reconnus lors du traitement, les fichiers de données

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

pouvant être agrégés et compressés au format '**gzip**'. L'utilitaire '**FWLogWatch**' intègre son propre mécanisme de résolution **DNS** doté d'un système de cache afin d'optimiser les performances lors du traitement de journaux volumineux.

Les fonctionnalités suivantes sont supportées :

- la génération d'une synthèse adaptative au format '**texte**' ou '**HTML**'. De nombreuses options facilitent la sélection et le regroupement automatique des informations présentées,
- la transmission automatique d'une notification contenant le nombre d'occurrences de l'évènement, les adresses IP source et destination, la référence de protocole et les ports source et destination via le script '**fwlw_notify**',
- la génération d'un rapport d'incident en mode interactif contenant l'ensemble des éléments nécessaires au suivi dont la création d'un numéro d'incident,
- la génération dynamique d'une règle de blocage de la tentative de connexion à l'origine de l'évènement sous la forme d'une règle au format '**IpChain**' via la script '**fwlw_response**',
- la surveillance en temps réel du fonctionnement par le biais d'un mini-serveur **WEB** embarqué dont l'accès est protégé par la présentation d'un couple identifiant/mot de passe.

On pourra regretter l'absence d'une fonction de recherche automatique du contact '**abuse**' ou '**IRT**' associé à l'adresse IP source lors de l'utilisation en mode 'interactif' (option '-i'), dont un exemple d'utilisation est proposé ci-dessous :

```
# fwlogwatch -i 300 -I /usr/local/etc/fwlogwatch.template
  fwlogwatch summary
  Generated Tue Dec 10 12:08:54 CET 2002 by root.
  1775 of 5887 entries in the file "/var/log/messages" are packet logs,
  339 have unique characteristics.
  First packet log entry: Dec 08 04:06:36, last: Dec 10 12:01:17.
  All entries were logged by the same host: "62.30.201.X".
  All entries are from the same chain: "Externe-Interne".
  All entries have the same target: "denied".
  Reporting threshold: 300

  (FastEthernet0/0 00a0.247c.ea18) 5785 packets from 62.30.201.X to 62.23.A.B
  ---------------------------------------------------------------------------
  From: support@veille.apogee-com.fr
  To: [Insert address of abuse contact or CERT here]
  Subject: Incident report 20021208-62.23.184.49

  Dear Madam or Sir,

  we would like to bring to your attention that [your organization's
  networks] have been subject to heavy scans from a/several host/s in
  your domain:

  Offending IP address:      62.30.201.X
  Target IP address:         62.23.A.B
  Number of logged attempts: 5785
  Tracking number:           20021208-62.30.201.X

  Please take the appropriate steps to stop these scans.
  In case you need more information we would be glad to provide you
  with the appropriate log file excerpts as far as they are available.

  Thank you.
  Yours sincerely

 [Your signature]
  ---------------------------------------------------------------------------
  Should this report be sent? [(s)end/(m)odify/(q)uit]
```

On veillera à ne pas pousser à l'extrême l'automatisation de ce processus de notification externe, un contrôle préalable de la raison d'être de la notification et des éléments transmis restant absolument nécessaire afin de rester courtois et de ne pas saturer le service de gestion des incidents de l'organisation distante par une information partielle, ou insuffisamment contrôlée. Le mode 'interactif' proposé par '**fwlogwatch**' doit être perçu comme une facilité de gestion et non comme une fonctionnalité d'automatisation.

En mode 'synthèse', le fonctionnement de '**fwlogwatch**' est simple mais très consommateur de ressources du moins si l'on conserve le principe original de fonctionnement en temps réel du script '**cgi-bin**' de consultation proposé en exemple. Lors de chaque connexion sur la page d'accès, ce script active la génération d'une synthèse au format 'HTML' puis dirige le navigateur vers la page d'index nouvellement produite.

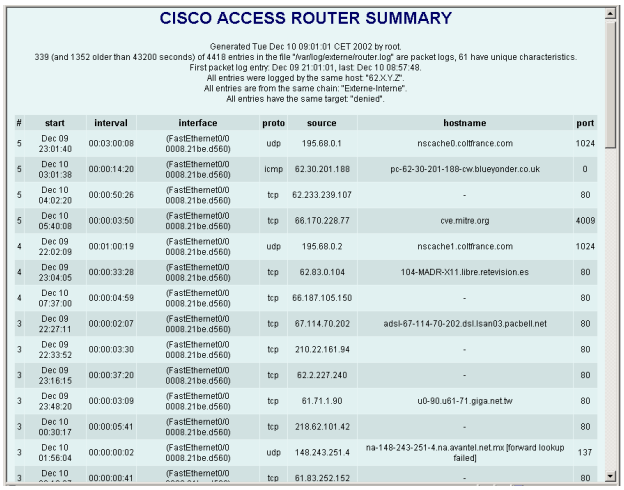
Nous suggérons une légère adaptation de ce mode de fonctionnement en confiant la génération des pages de synthèse à l'ordonnanceur '**cron**' sur la base d'une périodicité de l'ordre de l'heure, voire de la demi-heure. L'exploitant consultera simplement les résultats en dirigeant son navigateur, non plus sur le script 'cgi-bin' mais directement sur la page d'accueil régulièrement remise à jour.

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Nous utilisons depuis plusieurs mois cet outil rustique mais formidablement efficace pour visualiser les évènements correspondant au déclenchement des règles de sécurité du routeur protégeant l'accès à notre site de veille technologique.

Le résultat est plus que satisfaisant et l'effort d'installation de cet outil - dont nous rappelons qu'il est libre d'utilisation - est rapidement compensé par la pertinence des résultats et le gain de temps qui en découle.

La copie d'écran proposée ci-contre présente la synthèse mise à jour toutes les heures des événements détectés sur les dernières 24 heures. Les options de présentation ici employées autorisent une lecture rapide et efficace des évènements triés par nombre d'occurrence. Ici, la majorité des évènements portent sur les services **HTTP** et **NetBIOS**.



CISCO ACCESS ROUTER SUMMARY

Generated Tue Dec 10 09:01:01 CET 2002 by root.
339 (and 1352 older than 43200 seconds) of 4418 entries in the file "/var/log/external/router.log" are packet logs, 61 have unique characteristics.
First packet log entry: Dec 09 21:01:01, last: Dec 10 08:57:49.
All entries were logged by the same host: "62.X.Y.Z".
All entries are from the same chain: "Externe-Interne".
All entries have the same target: "denied".

#	start	interval	interface	proto	source	hostname	port
5	Dec 09 23:01:40	00:03:00:08	(FastEthernet0/0 0008.21be.d560)	udp	195.68.0.1	nscache0.colt.fr.ance.com	1024
5	Dec 10 03:01:38	00:00:14:20	(FastEthernet0/0 0008.21be.d560)	icmp	62.30.201.188	pc-62-30-201-188-cw.blueyonder.co.uk	0
5	Dec 10 04:02:20	00:00:50:26	(FastEthernet0/0 0008.21be.d560)	tcp	62.233.239.107	-	80
5	Dec 10 05:40:08	00:00:03:50	(FastEthernet0/0 0008.21be.d560)	tcp	66.170.228.77	cve.mitre.org	4009
4	Dec 09 22:02:09	00:01:00:19	(FastEthernet0/0 0008.21be.d560)	udp	195.68.0.2	nscache1.colt.fr.ance.com	1024
4	Dec 09 23:04:05	00:00:33:28	(FastEthernet0/0 0008.21be.d560)	tcp	62.83.0.104	104-MADR-X11.libre.retevision.es	80
4	Dec 10 07:37:00	00:00:04:59	(FastEthernet0/0 0008.21be.d560)	tcp	66.187.105.150	-	80
3	Dec 09 22:27:11	00:00:02:07	(FastEthernet0/0 0008.21be.d560)	tcp	67.114.70.202	adsl-67-114-70-202.dsl.lsan03.pacbell.net	80
3	Dec 09 22:33:52	00:00:03:30	(FastEthernet0/0 0008.21be.d560)	tcp	210.22.161.94	-	80
3	Dec 09 23:16:15	00:00:37:20	(FastEthernet0/0 0008.21be.d560)	tcp	62.2.227.240	-	80
3	Dec 09 23:48:20	00:00:03:09	(FastEthernet0/0 0008.21be.d560)	tcp	61.71.1.90	u0-90.u61-71.giga.net.tw	80
3	Dec 10 00:30:17	00:00:05:41	(FastEthernet0/0 0008.21be.d560)	tcp	218.62.101.42	-	80
3	Dec 10 01:56:04	00:00:00:02	(FastEthernet0/0 0008.21be.d560)	udp	148.243.251.4	na-148-243-251-4.na.avantel.net.mx [forward lookup failed]	137
3	Dec 10	00:00:00:41	(FastEthernet0/0	tcp	61.83.252.152	-	80

La version 0.9 actuellement disponible au téléchargement depuis le site de l'université de **Stuttgart** est stable depuis Août 2002.

Cette version fonctionne dans les environnements UNIX (Solaris, FreeBSD, OpenBSD) et Windows 32 par le biais de la librairie d'émulation **CygWin**.

- **Complément d'information**

http://cert.uni-stuttgart.de/projects/fwlogwatch/

LES TECHNOLOGIES

JAVA

LSDPL - JAVA ET LA SECURITE

- **Description**

Le célèbre groupe de spécialistes polonais de la sécurité dit '**LSD**' ou '**Last Stage of Delirium**' a dévoilé en octobre dernier à l'occasion de la conférence '**Asia BlackHat**' une remarquable étude de 85 pages intitulée '**Java and Java Virtual Machine Vulnerabilities and their Exploitation Techniques**'. Celle-ci nous offre une présentation magistrale des mécanismes fondamentaux mis en œuvre dans la technologie **JAVA** mais aussi des vulnérabilités associées.

Réservée au spécialiste du développement en environnement JAVA voire au curieux désireux de tout connaître du fonctionnement de la machine virtuelle Java (ou '**JVM**'), cette étude est divisée en 2 grands volets:

- Un rappel des spécificités originales du langage et de son support par un interpréteur spécialisé. Ce volet aborde notamment les fonctionnalités de sécurité spécifiques de cet environnement dont le procédé de vérification du code élémentaire dit '**Byte Code Verifier**', le modèle d'exécution contrôlée dit '**Applet SandBox Model**' ou encore le gestionnaire de sécurité dit '**Security Manager**'.
- Une présentation des vulnérabilités de conception mais aussi de réalisation présentes dans les différentes implémentations des machines virtuelles java. La lecture de ce volet requiert une excellente connaissance du langage mais aussi de l'implémentation de celui-ci dans la JVM pour comprendre les techniques d'attaques mises en œuvre.

On retiendra de cette étude la complexité – mais aussi l'élégance - des solutions de contournement des mécanismes de sécurité qui toutes interviennent au plus bas niveau de l'interprétation du code élémentaire **Java**, le Byte Code. On notera qu'en dehors de problèmes inhérents à la définition même du langage et à son implémentation, plusieurs failles trouvent leur origine dans l'interface de cette implémentation – la JVM - avec les mécanismes natifs du système généralement accédés par le biais de librairies pouvant ne pas respecter les mêmes conventions de représentation des données ou de passage des paramètres. Le lecteur intéressé par ce problème pourra se reporter à l'excellent article '**Perl CGI problems – Poison NULL byte**' publié dans le numéro **55** de la revue **Phrack**.

Nous avons particulière apprécié la présence en annexe B d'un tableau comparatif des spécificités des implémentations **NetScape** et **Microsoft** du **Java Security Manager** – le composant responsable de la validation du code et de l'autorisation des actions dans le contexte d'exécution.

L'annexe C nous offre un intéressant historique de la découverte des principaux bogues de conception et d'implémentation mis en évidence de février 1996 à nos jours, soient les 19 bogues référencés comme suit :

1996	Février	**DNS Spoofing attack**	Corrigé dans la VM SUN JDK1.01 et le navigateur Netscape 2.02
	Mars	**Class loader**	Corrigé dans la VM SUN JDK1.02 et le navigateur Netscape 2.02
	Mars	**Byte code verifier**	Corrigé dans la VM SUN JDK1.02 et le navigateur Netscape 2.02
	Avril	**Hostile applets**	Code écrit principalement pour le navigateur Netscape 3.0
	Mai	**Class loader variant**	VM SUN et le navigateur Netscape

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	Juin	**Illegal type cast**	Corrigé dans la VM SUN JDK1.1, navigateurs Netscape 3.0, IE4.0
1997	Mars	**VM bug**	Corrigé dans la VM SUN JDK1.1.2
	Avril	**Signing flaw**	Corrigé dans la VM SUN JDK1.1.2 et le navigateur HotJava
	Mai	**Kimera verifier bug**	Corrigé dans la VM SUN JDK1.1
1998	Juillet	**Princeton Class loader**	Corrigé dans la VM SUN JDK1.2 et le navigateur Netscape 4.5
1999	Mars	**Verifier bug**	Corrigé dans la VM SUN JDK1.1.8 et le navigateur Netscape 4.51
	Avril	**Unverified code**	Corrigé dans la VM SUN JDK1.1.8
	Août	**Loading race condition**	Découvert dans la VM livrée avec les navigateurs IE 4.01 et 5.0
	Octobre	**Verifier bug**	Corrigé dans le navigateur IE 5.5 et les VM associés suivantes
2000	Février	**VM reading vuln.**	Découvert dans la VM livrée avec les navigateurs IE 4.x et 5.x
	Août	**Brown orifice exploit**	Corrigé dans le navigateur Netscape 4.75
	Octobre	**VM ActiveX Component**	Découvert dans la VM livrée avec navigateurs IE 4.x et 5.x
	Novembre	**Class loading issue**	Identifié dans les VM SUN JDK1.1.x et 1.2.x, détails non publiés
2002	Mars	**Byte code verifier**	Corrigé dans le navigateur Netscape 6.2.2, Java 2 SDK, JVM v1.4

Rappelons que le langage **JAVA** reste remarquablement positionné sur le marché, et ce malgré la présence de concurrents sérieux dont la technologie '**.NET**'.

Le nombre de dispositifs utilisant la technologie Java ne cesse de croître : téléphones mobiles, assistants personnels et même cartes à puces embarquent désormais un interpréteur **JAVA**. De la sécurité et de la fiabilité de celui-ci dépend désormais une grande quantité d'applications commerciales …

A ce propos, notons que les auteurs considèrent que le principal vecteur de menace reste la téléphonie mobile dont la plate-forme JAVA '**iAppli**' embarquée dans la technologie '**Docomo**' développée par **NTT** et actuellement plus connue en France sous l'appellation '**imode**' …

1 **Introduction**
2 **Java language security features**
3 **The applet sandbox**
4 **JVM security architecture**
  4.1 Class Loader
  4.2 The Bytecode Verifier
  4.3 Security Manager
5 **Attack techniques**
  5.1 Type confusion attack
  5.2 Class Loader attack (class spoofing)
  5.3 Bad implementation of system classes
6 **Privilege elevation techniques**
  6.1 Netscape browser
  6.2 MSIE browser
7 **The unpublished history of problems**
  7.1 JDK 1.1.x
  7.2 MSIE 4.01
  7.3 MSIE 4.0 5.0
  7.4 JDK 1.1.x 1.2.x 1.3 MSIE 4.0. 5.0. 6.0
8 **New problems**
  8.1 JIT Bug (Netscape 4.x)
  8.2 Verifier Bug (MSIE 4.0 5.0 6.0)
  8.3 Verifier Bug (Netscape 4.x)
  8.4 Insecure functionality (Netscape 4.x)
9 **JVM security implications**
A **The Bytecode verification**
B **Comparison of Security Manager Implementations**
C **The Brief History of Java Bugs**

▪**Complément d'information**

http://www.lsd-pl.net/java_security.html
http://www.blackhat.com/html/bh-asia-02/bh-asia-02-index.html
http://www.eurotechnology.com/imode/faq-java.html

ASP.NET

MICROSOFT – BUILDING SECURE ASP.NET APPLICATION

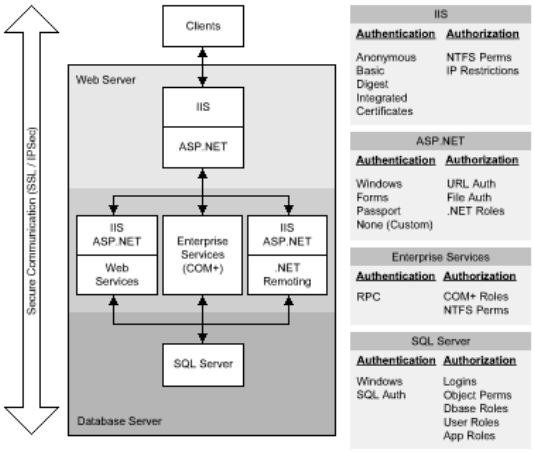
▪**Description**

Véritable bible de plus de 608 pages accessible gratuitement aux formats '**HTML**' et '**PDF**', cet ouvrage intitulé '**Building Secure ASP.NET Applications**' est destiné à inculquer les fondements de la conception et de la programmation des applications **ASP.NET** dans le cadre de l'environnement de développement '**.NET**' (version 1.0).

Les thèmes fondamentaux abordés dans ce guide sont mis en exergue par le sous-titre retenu : '**Authentication, Authorization and Secure Communications**'.

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Plus précisément, cet ouvrage aidera le concepteur ou le développeur à mettre en place les procédés permettant d'identifier les clients des applications (Authentication), de contrôler finement l'accès aux ressources mises à disposition par les celles-ci (Authorization) et enfin à garantir que les messages échangés entre le client et l'application resteront confidentiels et intègres.



Un vaste programme s'il en est dont la mise en œuvre dictera la qualité du service rendu aux clients de l'entreprise par l'entremise de la technologie .**NET**, certes prometteuse mais dont la complexité rebute plus d'un développeur.

La position respective de chacun des composants participant à l'architecture '**ASP.NET'** en matière de sécurité est parfaitement récapitulée par le synoptique ci-contre, extrait de l'ouvrage.

Ce guide a le mérite de couvrir l'ensemble des thèmes clefs en faisant preuve d'une pédagogie rarement rencontrée en matière de sécurité mais suppose cependant de disposer d'un minimum de culture en matière de programmation dans l'environnement '**Visual .NET**' et surtout d'une bonne connaissance de la logique développée par Microsoft.

Pour les lecteurs qui l'ignoreraient, le terme '**ASP.NET**' résulte de la contraction de deux sigles :

1- '**ASP**' – **Active Server Page** - désignant la technologie développée il y a déjà quelques années par Microsoft pour gérer un contenu dynamique en environnement Internet Information Server. Cette technologie s'appuyait sur une variation du langage Visual Basic adaptée au contexte de la génération de page.

2- '.**NET**' désignant le tout dernier environnement de développement conçu par Microsoft pour les langages C# (prononcez 'C SHARP'), Visual Basic et JScript. Il s'agit de ce que l'on appelle dans le jargon un 'framework réseau' offrant l'accès à toutes les objets et ressources de l'infrastructure Microsoft, que ceux-ci soient localisés sur le poste de travail, sur le réseau de l'entreprise ou dans un quelconque lieu de stockage sur l'Internet.

Nos lecteurs souhaitant approfondir ce domaine peuvent consulter avec profit la page '**Tutorial**' du site 'http://www.asp.net' dédié à cette technologie.

Un extrait de la table des matières de cet ouvrage est proposé ci-dessous à titre d'information:

Part I, Security Models
Chapter 1: Introduction
Chapter 2: Security Model for ASP.NET Applications
Chapter 3: Authentication and Authorization
Chapter 4: Secure Communication
Part II, Application Scenarios
Chapter 5: Intranet Security
Chapter 6: Extranet Security
Chapter 7: Internet Security
Part III, Securing the Tiers
Chapter 8: ASP.NET Security
Chapter 9: Enterprise Services Security
Chapter 10: Web Services Security
Chapter 11: Remoting Security
Chapter 12: Data Access Security
Part IV, Reference
Chapter 13: Troubleshooting Security
How Tos
Base Configuration
Configuration Stores and Tools
Reference Hub
How Does It Work?
ASP.NET Identity Matrix
Cryptography and Certificates
.NET Web Application Security
Glossary

Remarquablement organisé et présenté, cet ouvrage répond à toutes les questions que l'on est droit de se poser quand à la sécurité d'une infrastructure fondamentalement répartie et coopérative. Deux chapitres méritent une lecture attentive:

- Le chapitre '**At a glance**' situé en introduction de l'ouvrage récapitule avec force de graphiques, le contenu et les objectifs des 13 chapitres suivants. Sa lecture est conseillée à qui souhaite disposer d'une vue d'ensemble des principes fondamentaux de la technologie '**ASP.NET**',
- Le chapitre '**HowTos**' regroupant quelques 20 questions que se posent souvent les développeurs dont les techniques d'indexation, la création d'un compte spécifique, l'utilisation de formulaires d'authentification, l'utilisation de la délégation **Kerberos**, d'**IPSEC** … en un mot, un mine de renseignements pour tout développeur voire même pour l'exploitant d'une infrastructure basée sur la technologie '**ASP.NET**'.

▪**Complément d'information**

http://msdn.microsoft.com/library/en-us/dnnetsec/html/secnetlpMSDN.asp

http://download.microsoft.com/download/VisualStudioNET/Security/RTM/NT5/EN-US/secnet.exe

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

INCIDENTS

CSIRT – LES SERVICES

▪**Description**

Le terme '**CERT**' – **C**omputer **E**mergency **R**esponse **T**eam – longtemps utilisé comme sigle générique désignant une organisation en charge de la gestion des incidents de sécurité cède peu à peu sa place au terme **CSIRT**' – **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam - libre de tous droits et adopté de longue date par la communauté Européenne, et en particulier dans le cadre du programme '**TERENA**'. Rappelons en effet que les sigles '**CERT**' et '**CERT Coordination Center**' sont des marques propriétés de l'université de **Carnegie-Mellon** et ne peuvent donc être librement utilisées.

Effet du hasard ou contrepartie de l'actualité et des programmes nationaux de sécurité, un net regain d'intérêt et d'activité est constaté autour du thème de la gestion des incidents et de l'organisation des équipes d'intervention, que cela soit le fait d'organismes étatiques ou de sociétés purement commerciales cherchant à valoriser leurs services.

Citons ainsi '**Symantec**' et son programme d'alerte avancée (DeepSight Alert Services) mais aussi les sociétés de conseil hollandaise **STELVIO** (chargé de la gestion et de l'habilitation des **CSIRT** en Europe) et allemande **PRESECURE** (œuvrant dans le domaine de l'assistance et de la formation) ou encore notre propre société avec ses services d'alerte et de veille technologique.

Face à la confusion pouvant être provoquée par les différentes dénominations employées pour désigner des services en pratique identiques, le **CERT-CC** et les sociétés pré-citées **STELVIO** et **PRESECURE** ont édité un document succinct mais fort intéressant car proposant une classification des services susceptibles d'être proposés par un '**CSIRT**'.

Nous reproduisons ci-dessous la table de description des services identifiés dans ce document intitulé '**CSIRT Services**', ceux étant classés en trois catégories :

Services réactifs - Réponse à un incident	
Alertes et notifications	**Alerts and Warnings**
Gestion des incidents Analyse de l'incident Traitement sur site Assistance suite à incident Coordination de l'action	**Incident handling** Incident analyse Incident response on site Incident response support Incident response coordination
Gestion des vulnérabilités Analyse de vulnérabilité Traitement de l'incident Coordination de l'action	**Vulnerability handling** Vulnerabiliy handling Vulnerability response Vulnerability response coordination
Gestion des artéfacts Analyse de l'artéfact Traitement de l'incident Coordination de l'action	**Artefact handling** Artefact handling Artefact response Artefact response coordination

Services proactifs - Prévention de l'incident	
Annonces	**Announcements**
Veille technologique	**Technology watch**
Audit et validation de sécurité	**Security Audit or Assessments**
Configuration et maintenance des outils de sécurité, des applications et infrastructures	**Configuration & maintenance of security tools, applications & infrastructures**
Détection d'intrusion	**Intrusion Detection Services**
Contrôle de la diffusion des informations	**Security Related information Dissemination**

Qualité de la sécurité - Maintenance du service	
Analyse de risque	**Risk analysis**
Plan de secours	**Business continuity & Disaster recovery planning**
Conseil	**Security consulting**
Sensibilisation	**Awareness building**
Education / Formation	**Education / Training**
Evaluation ou Certification des produits	**Product Evaluation or Certification**

Cette classification fait apparaître une catégorie de services dont il faut avouer qu'elle n'est pas encore très répandue du moins commercialement en Europe : **l'analyse d'artefact**, c'est à dire d'objets informatiques manufacturés – fichiers, messages, exécutables, … - découverts dans un système d'information et dont le rôle n'est pas explicitement

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

connu de l'exploitant. Lorsque l'on sait le nombre de fichiers exécutables inconnus quotidiennement découverts sur les serveurs d'une importante infrastructure et non répertoriés dans les bases de référence des mécanismes anti-virus, on ne peut qu'envisager un fort développement de ce genre d'activité à court terme.
Ce document vient à propos pour éclaircir le rôle et les actions dévolues à un '**CSIRT**', certaines d'entre-elles pouvant d'ailleurs être sous-traitées.

- **Complément d'information**

http://www.cert.org/csirts/services.html
http://www.stelvio.nl/
http://www.pre-secure.com

CERT – TRACER LES ATTAQUES

- **Description**

Le **CERT-CC®** met à disposition un état de l'art de 37 pages portant sur les procédés et techniques permettant de tracer l'origine d'une attaque et de remonter aux sources de celle-ci.

Un premier volet aborde les problèmes à l'origine de la difficulté rencontrée pour retrouver l'origine réelle d'une attaque. Parmi les 12 raisons évoquées, deux justifications sont plus particulièrement à prendre en compte : l'Internet n'a jamais été conçu pour remonter à l'origine d'une connexion et son extension planétaire entre en conflit avec les intérêts et contraintes locales ou nationales.

Le second volet, particulièrement technique, retrace les différents procédés palliatifs mis au point pour parer à l'absence de toute fonction de tracabilité fiable. En pratique, si la majorité de ces procédés permettront de déterminer le(s) point(s) d'entrée d'une attaque dans l'infrastructure gérée par le **FAI**, tous nécessiteront cependant une coopération à plus vaste échelle pour aller au-delà des frontières administratives et nationales. Diverses méthodes et techniques heuristiques en cours d'étude sont présentées dont aucune hélas ne répondra aux attentes pratiques des exploitants et services spécialisés dans l'investigation des 'cyber-attaques'.

Part I: Technical Challenges in Tracking and Tracing Cyber-Attacks

1 Introduction
2 A Brief History of the Internet
3 A Brief Tutorial on Internet Technology
4 Problems with Internet Security
5 Shortfalls in the Current Internet Environment
5.1 The Internet was never designed for tracking and tracing user
5.2 The Internet was not designed to resist highly untrustworthy users
5.3 A packet's source address is untrustworthy, which severely hinders
5.4 The current threat environment far exceeds the Internet's design
5.5 The expertise of the average system administrator continues to
5.6 Attacks often cross multiple administrative, jurisdictional, and national
5.7 High-speed traffic hinders tracking
5.8 Tunnels impede tracking
5.9 Hackers destroy logs and other audit data
5.10 Anonymizers protect privacy by impeding tracking
5.11 The ability to link specific users to specific IP addresses is being lost
5.12 Purely defensive approaches will fail, so deterrence through tracking
6 Example: A "Smurf" IP Denial-of-Service Attack

Part II: Promising Research Approaches: The Search for Near- andLong-Term Solutions

7 Overview
8 Basic Approaches
8.1 Hop-by-Hop IP Traceback
8.2 Ingress Filtering
8.3 Policy Implications
9 Backscatter Traceback
9.1 Comments on the Backscatter Traceback Technique
9.2 Policy Implications
10 An Overlay Network for IP Traceback
10.1 Comments on the CenterTrack Method
11 Probabilistic Approaches to Packet Tracing
11. 1 Generating Trace Packets (Using Control Messages)
11. 2 Packet Marking Schemes
11. 3 Comment on Probabilistic Traceback Approaches
11. 4 Policy Implications
12 Single-Packet IP Traceback
12.1 Comments on the Hash-Based Traceback Approach
12.2 Policy Implications
13 Policy Considerations
13.1 Intense International Cooperation is Essential
13.2 Migrating Critical Applications to the Internet
13.3 Privacy
13.4 Incorporate Policy into Automated Tracking, Recovery, and Response
13.5 Imprecise Jurisdictional Boundaries
13.6 Levels of Evidence
13.7 Levels of Damage and Threat
13.8 Liability Issues
13.9 Honeypots and Honeynets
14 Technical and Policy Requirements for Next-Generation Internet Protocols

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

14.1 Background
14.2 The "Entry-Point Anonymity" Problem
14.3 Vigilant Resource Consumption
14.4 Trust Management and Privacy
14.5 "Situation-Sensitive" Security and Trust Processing
14.6 Sufficient Header Space for Tracking Information
14.7 Emerging Next-Generation Security Protocols
15 Conclusion
Bibliography

La lecture de cette excellente étude intéressera en priorité les administrateurs de plaques réseaux importantes, **FAI** mais aussi sociétés commerciales disposant de leur propre infrastructure.

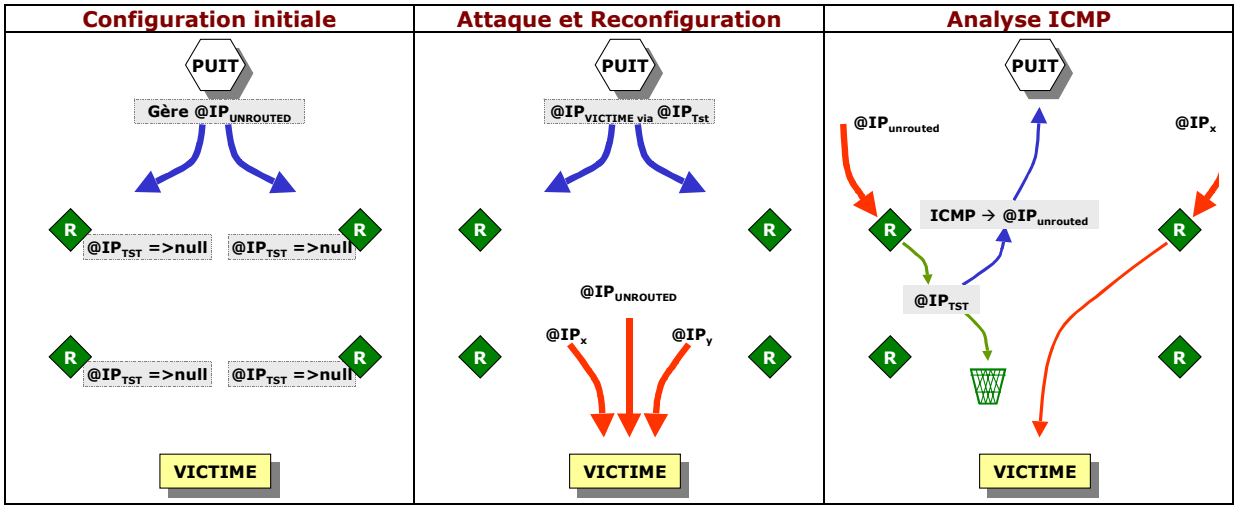
Pour mieux comprendre les techniques d'identification de la source et en particulier celle dite du '**Backscatter Traceback**', nous préconisons la lecture de l'excellent document publié par **CISCO** à l'attention des FAI.

La procédure pratique proposée par **CISCO** pour mettre en œuvre cette technique repose sur plusieurs hypothèses et mécanismes de routage dont

1- la possibilité de router un paquet sur une interface 'nulle', opération générant un message **ICMP** '**Unreachable**' vers l'adresse IP annoncée en tant que source dans le paquet. En pratique, tous les routeurs de l'infrastructure sont configurés pour router les adresses d'un réseau non utilisé – le réseau de TEST **192.0.2.0/24** par exemple - vers le port '**null0**' du routeur. Tout paquet reçu à destination de ce réseau sera en conséquence immédiatement détruit, la source étant informée du problème par le message ICMP '**Unreachable**'. Ce message contient notamment l'adresse IP du routeur ayant effectué l'opération,

2- l'utilisation du protocole de routage interne dit '**iBGP**' permettant de modifier conditionnellement la route menant vers la victime de l'attaque en annonçant comme prochain saut une adresse située dans le réseau configuré pour être absorbé, dans notre exemple, le réseau TEST. Sur détection d'une attaque, une reconfiguration de la route est engagée puis propagée. Les paquets à destination de la victime sont alors absorbés sur l'équipement au plus prés de la bordure de l'infrastructure qui génère alors le message **ICMP** 'Unreachable' contenant son adresse à destination de la source.

3- la mise en place d'un routeur '**Puit**' annonçant qu'il gère plusieurs blocs d'adresses IP non alloués dans l'Internet, et non utilisés dans l'infrastructure concernée. En considérant que la majorité des attaques utilisent une adresse source forgée et que celle-ci appartienne avec une bonne probabilité à un bloc d'adresses non alloué, les messages ICMP 'Unreachable' transmis en retour vers ces adresses seront automatiquement dirigés vers le routeur 'Puit'. Celui-ci pourra alors acquérir l'adresse IP des routeurs situés en bordure de l'infrastructure ayant routé les paquets d'attaque.



▪**Complément d'information**

http://www.cert.org/archive/pdf/02sr009.pdf

http://www.cisco.com/public/cons/isp/security/K_Traceback_v2-3.pdf

CRYPTOGRAPHIE

ECCP-109 – DEFI REMPORTE

▪**Description**

Le 6 novembre, la société **CertiCom** a révélé qu'une équipe de l'université Notre Dame – Ontario – avait remportée l'un des deux défis cryptographiques **ECCp** lancés en 1997. Destinés à démontrer la robustesse de la technologie de cryptographie dite à courbes elliptiques - **ECC** (Elliptic Curve Cryptosystem) , ces défis consistaient à calculer une clef privée de respectivement 109 et 131 bits à partir d'un ensemble de clefs publiques et des paramètres ECC associés. La seconde phase du défi portera sur des tailles de clefs privées de 163, 191, 239 et 359 bits !

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

La société **CertiCom** a toujours considéré que les défis de la première phase restaient solvables en l'état de la technologie avec une estimation initiale de quelques mois pour la clef de 109 bits et considérablement plus pour la seconde. En pratique, il aura fallu la puissance combinée de quelque 10 000 ordinateurs, pour la plupart des PC sur une durée de 549 jours de calcul intensif pour venir à bout du défi **ECCp-109**.

Le défi précédent, **ECC2K-108**, portant sur une clef **ECC** de 108 bits et remporté en Avril 2000 (Rapport N°21 – Avril 2000) par une équipe Française de l'INRIA, avait nécessité 9500 ordinateurs et environ 4 mois de calculs intensifs. La puissance de calcul alors requise était 50 fois plus importante que celle mise en œuvre pour résoudre le challenge RSA-512 conduisant **CertiCom** à communiquer sur la robustesse de la technologie ECC actuellement utilisée avec des clefs de 163 bits.

▪**Complément d'information**

http://www.certicom.com/about/pr/02/021106_ecc_winner.html

SECURISATION

NSA - GUIDE TO SECURING MICROSOFT INTERNET EXPLORER 5.5 USING GROUP POLICY

▪**Description**

Daté de juillet 2002 et mis à disposition fin novembre, ce nouveau guide de 49 pages publié par la **NSA** décrit la mise en œuvre du mécanisme des **GPO** (Group POlicy) pour sécuriser Internet Explorer version 5.5. Le cas de la version 6.0 – la dernière en date – est traité sous la forme d'un chapitre dédié livré en annexe et décrivant par le détail les options et paramètres spécifique à cette nouvelle version du navigateur.

En introduction, l'auteur de ce guide énonce les 4 règles fondamentales qu'un navigateur devra respecter pour être considéré correctement configuré, ou plus précisément, pour être configuré le plus sûrement possible sans entraver le son fonctionnement dans le contexte professionnel.

Règle N°1	Aucune requête n'est effectuée par le navigateur qui ne soit le résultat d'une requête effectuée par l'utilisateur.
Règle N°2	Les informations envoyées vers un site WEB par le navigateur doivent être maintenues dans un contexte associé à ce site sauf mention explicite de l'utilisateur.
Règle N°3	Le navigateur doit offrir des canaux de communication garantis vers les sites WEB quand cela est requis. De tels canaux sont clairement identifiés ainsi que le site situé à leur extrémité.
Règle N°4	Tout script ou programme exécuté par le navigateur le sera dans un environnement restreint. Les programmes délivrés par des canaux garantis pourront être autorisés à quitter cet environnement.

Plusieurs options de configuration peuvent être sélectionnées qui permettent de respecter ces 4 règles fondamentales. Dans l'optique de faciliter la mise en œuvre de la configuration, l'auteur a choisi de regrouper toutes les options de configuration interdépendantes au sein d'un même et unique groupe et de proposer plusieurs profils de configuration pour chacun des 4 groupes ainsi définis:

Groupe A	**Autorisation d'exécution des contrôles ActiveX et des 'plug-ins'**
Groupe B	**Autorisation d'installation des contrôles ActiveX**
Groupe C	**Autorisation de téléchargement de fichier par l'utilisateur**
Groupe D	**Gestion et traitement des connexions réseaux**

Pour chaque groupe, l'administrateur devra sélectionner le profil de configuration le plus adapté à son contexte, s'y tenir et appliquer les paramètres de configuration associés tout au long du processus décrit dans les chapitres suivants : chapitre 3 portant sur les paramètres accessibles depuis Internet Explorer et chapitre 4 détaillant les paramètres complémentaires applicables depuis la **MMC** (Microsoft Management Console) par le biais d'un modèle '**.adm**'.

Le lecteur trouvera ci-après un extrait de la table des matières proposé à titre d'information:

CHAPTER 1: INTRODUCTION
CHAPTER 2: LINKED DECISIONS
ABOUT ACTIVEX CONTROLS
LINKED DECISION GROUP A: WHO CAN RUN ACTIVEX CONTROLS AND PLUG-INS?
Option A1: Only Allow Trusted Sites to Run ActiveX Controls and Plug-ins
Option A2: Allow All Sites to Run ActiveX Controls marked "Safe for Scripting" and Plug-ins (Recommended)
LINKED DECISION GROUP B: WHO CAN INSTALL ACTIVEX CONTROLS?
Option B1: Do Not Allow ActiveX Control Installation (Recommended)
Option B2: Allow Trusted Sites to Install ActiveX Controls
Option B3: Allow ActiveX Controls to be Installed from Approved Cache
Option B4: Allow ActiveX Controls based on Authenticode Certificate
LINKED DECISION GROUP C: WHAT FILES CAN USERS DOWNLOAD?
Option C1: Do not allow file download, only allow viewing by plug-in (Recommended)
Option C2: Allow opening files but disallow saving them
Option C3: Allow all file downloads
LINKED DECISION GROUP D: ARE NETWORK CONNECTION SETTINGS A SECURITY CONCERN?
Option D1: Network Settings should be set now (Recommended)
Option D2: Network Settings should be hidden but not set
Option D3: Network Settings should be changeable by the user
CHAPTER 3: GROUP POLICY SETTINGS PROVIDED BY MICROSOFT
SETTINGS IN THE "COMPUTER" AREA
Security Zones: Use only machine settings, Do not allow users to change policies, Do not allow users to add/delete sites
Make proxy settings per-machine (rather than per-user)
Disable Automatic Install of Internet Explorer components

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

SETTINGS IN THE WINDOWS SETTINGS PORTION OF THE "USER" AREA
Connection Settings
Security Zones and Content Ratings
Authenticode Settings
SETTINGS IN THE ADMINISTRATIVE TEMPLATE PORTION OF THE "USER" AREA
Internet Control Panel
Offline Pages
Browser Menus
Administrator Approved Controls
Disable Changing Advanced Page Settings, Certificate Settings, Automatic Configuration Settings, Internet Connection Wizard, Changing Connection Settings, Changing Proxy Settings
Do not allow AutoComplete to save passwords
CHAPTER 4: GROUP POLICY SETTINGS PROVIDED BY ADM TEMPLATE
REGISTRY SETTINGS UNDER HKEY CURRENT USER
Checking for Certificate Revocation
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is closed
Use Fortezza
Cryptographic Protocols
Warn About Invalid Certificates, Warn if forms submittal is being redirected
Disable Password Caching
REGISTRY SETTINGS UNDER HKLM
Controlling Sources of ActiveX Downloads
APPENDIX A: SECURITY SETTINGS BY ZONE
ACTIVEX CONTROLS
Download Signed ActiveX Controls, Download Unsigned ActiveX Controls
Initialize and Script ActiveX Controls Not Marked as Safe
Run ActiveX Controls and Plug-ins
Script ActiveX Controls Marked Safe for Scripting
COOKIES
Allow Per Session Cookies
Allow Cookies That Are Stored On Your Computer
DOWNLOAD
File Download
Font Download
JAVA
Java Permissions
MISCELLANEOUS
Access Data Sources Across Domains
Don't Prompt for Client Certificate Selection When No Certificates or Only One Certificate Exists
Drag and Drop or Copy and Paste Files
Installation of Desktop Items
Launching Applications and Files in IFRAME
Navigate Sub-Frames Across Different Domains
Software Channel Permissions
Submit Non-Encrypted Form Data
UserData Persistence
SCRIPTING
Active Scripting
Allow Paste Operations Via Script
Scripting Java Applets
USER AUTHENTICATION
Logon
APPENDIX B: DIFFERENCES IN CONFIGURING INTERNET EXPLORER 6.0
NEW SECURITY ZONE OPTIONS
Meta Refresh
Display Mixed Content
NEW ADVANCED PAGE OPTIONS
Enable 3 rd Party Browser Extensions
Check for Signatures on Downloaded Programs
NEW PRIVACY OPTIONS
APPENDIX C: ADM FILES
APPENDIX D: INTERNET EXPLORER AND GROUP POLICY REFERENCES
APPENDIX E: CONFIGURATION SUMMARY WORKSHEETS
Worksheet 1: Group Policy Settings Provided By Microsoft
Worksheet 2: Security Settings By Zone
Worksheet 3: Group Policy Settings Provided by ADM Templates

Nous avons particulièrement apprécié l'organisation de ce guide autorisant une mise en œuvre facilitée par la présence de 3 tableaux récapitulatifs en fin de document. On regrettera cependant que ces tableaux ne soient pas accessibles au format original, à savoir le format '**EXCEL**'.

Chaque élément de configuration fait l'objet d'une présentation détaillée parfois plus précise que celle proposée par l'éditeur. On notera à ce propos la présence de diverses informations fort utiles de toute évidence issues de l'expérience pratique de l'auteur et des équipes du **SNAC** (**S**ystem and **N**etwork **A**ttack **C**enter).

Ce guide devra faire l'objet d'une légère adaptation dans le cas d'une mise en œuvre dans une infrastructure utilisant une version francisée d'Internet Explorer, les paramètres de configuration accessibles depuis l'interface du navigateur étant référencés sous leur dénomination Anglo-saxonne.

- **Complément d'information**

http://svcaacs.conxion.com/support/guides/sd-8.pdf

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

NSA - GUIDE TO SECURING MICROSOFT WINDOWS XP

▪**Description**

Ce guide de sécurisation de 129 pages est entièrement consacré à la dernière mouture des systèmes d'exploitation de Microsoft: Windows™ XP. Il vient compléter fort à propos la série des guides déjà diffusés par la **NSA** portant sur Windows™ NT et Windows™ 2000. On notera l'avertissement des auteurs en introduction qui précisent que ce guide ne s'intéresse qu'à la sécurisation des postes utilisant la version dite '**professionnelle**' sous réserve que ces postes soient membres d'un domaine Windows 2000 dans lequel le service Active Directory aura été déployé. Les procédés de sécurisation font en effet appel aux mécanismes de gestion des politiques de groupe (**GPO**).

Plus précisément, la mise en œuvre de ce guide suppose que les hypothèses suivantes soient vérifiées dont certaines sont fortement 'réductrices' notamment dans le cas d'une infrastructure préexistante :

1-L'infrastructure est uniquement constituée de postes fonctionnant sous **Windows™ 2000** ou **XP** professionnel fraîchement installés, c'est à dire n'ayant pas fait l'objet d'une migration depuis une version antérieure,

2-Les derniers 'service packs' et correctifs Windows 2000 et XP sont installés sur l'ensemble des postes de l'infrastructure concernée,

3-Les contrôleurs de domaine fonctionnent tous sous **Windows™ 2000**, le service **ADS** devant être actif sur ceux-ci,

4-Les postes Windows™ XP sont formatés en utilisant le système de fichiers '**NTFS**',

5-L'architecture INTEL est utilisée sur tous les postes,

6-Les applications sont toutes compatibles **Windows™ XP**.

On notera l'implication de l'hypothèse N°1 concernant l'absolue nécessité de disposer de postes fraîchement installés conduisant en conséquence à devoir considérer privilégier la réinstallation systématique à la migration. La problématique de la migration sécurisée d'une version à l'autre est décidément loin d'être résolue en environnement Windows.

Le lecteur trouvera ci-dessous à titre d'information un extrait de la table des matières :

Chapter 1 Important Information on Using this Guide
Assumptions
Warnings to Review Before Using this Guide
Conventions and Commonly Used Terms
About the Guide to Securing Microsoft Windows XP
Chapter 2 What's New in Windows XP Security
Changes to Security Features
New Security Features
Chapter 3 Introduction to the Security Configuration Manager Tools
Security Configuration Functionality.
Security Templates
Before Making Security Changes
Checklist for Applying the Recommendations in this Guide
Chapter 4 Modifying Account Policy Settings with Security Templates
Password Policy
Account Lockout Policy
Kerberos Policy
Chapter 5 Modifying Local Policy Settings with Security Templates
Auditing Policy
User Rights Assi
Security Options
Adding an Entry to Security Options
Chapter 6 Modifying Event Log Settings with Security Templates
Event Log Settings
Managing the Event Logs
Chapter 7 Managing Restricted Groups with Security Templates
Modifying Restricted Groups via the Security Templates Snap-in
Chapter 8 Managing System Services with Security Templates
Modifying System Services via the Security Templates Snap-in
System Services Security
Chapter 9 Modifying Registry Security Settings with Security Templates
Inheritance model
Registry permissions
Registry settings via the Security Templates snap-in
Recommended Registry Key Permissions
Chapter 10 Modifying File System Security Settings with Security Templates
Converting to NTFS
File and folder permissions
Modifying File System settings via the Security Template snap-in
Recommended File and Folder Permissions
Chapter 11 Security Configuration and Analysis
Loading the Security Configuration and Analysis Snap-in into the MMC
Security Configuration Databases
Secedit Command Line Options
Configuring a System
Chapter 12 Applying Windows XP Group Policy in a Windows 2000 Domain
Overview
Security Settings Extension
Creating a Window XP GPO
Importing a Security Template into a GPO

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Managing a Windows XP GPO from a Windows 2000 Domain Controller
Local Group Policy Object
Forcing a Group Policy Update
Viewing the Resultant Set of Policy
Known Issues
Chapter 13 Remote Assistance/Desktop Configuration
Remote Assistance
Remote Desktop Connections
Group Policy – Administrative Templates
Network Configuration Recommendations
Chapter 14 Internet Connection Firewall Configuration
Recommended Usage
Features
Enabling the ICF
Summary
Chapter 15 Additional Security Settings
Administrator Accounts Recommendations
Shared Resource Permissions
Deleting POSIX Registry Keys
Additional Group Policy Settings
Blocking NetBIOS at the Network Perimeter
Chapter 16 Modifications for Windows XP in a Windows NT Domain
Lack of GroupPolicy
NTLM and LanManager Settings
Strong Session Key
Autoenrollment
Appendix A Example Logon Banner
Appendix B References

Nous recommandons fortement la lecture attentive de ce remarquable - mais dense – document à toute personne souhaitant disposer d'une approche pragmatique et fiable des procédés et mécanismes de sécurité intégrés au système **Windows™ XP**. La lecture du chapitre 2, et notamment du paragraphe '**New Security Features**', est absolument indispensable à qui souhaite disposer d'une liste synthétique – moins de 3 pages d'informations cruciales – des évolutions du modèle et des fonctions de sécurité.

- **Complément d'information**

http://svcaacs.conxion.com/winxp/guides/wxp-1.pdf
http://svcaacs.conxion.com/winxp/guides/inf/workstation.inf

NSA - CATALOGUE DES GUIDES DE SECURITE

- **Description**

La parution de deux nouveaux guides de sécurisation nous amène à proposer une mise à jour de notre catalogue qui liste ces documents en mettant en évidence le thème de rattachement, le titre, le numéro de révision et la date de publication.
Les codes suivants y sont utilisés :

I Document d'information et/ou de synthèse
G Guide de mise en œuvre et/ou manuel d'utilisation
R Recommandations et principes élémentaires
P Procédures et mise en application
✓ Document récemment mis à jour
✎ Document nouvellement publié

Windows XP

Système

✎	G	**Guide to Securing Microsoft Windows XP**	**V1.0**	30/10/2002	01

Windows 2000

Références

	I	**Microsoft Windows 2000 Network Architecture Guide**	**V1.0**	19/04/2001	01
	I	**Group Policy Reference**	**V1.08**	02/03/2001	04

Système

	G	**Guide to Securing Microsoft Windows 2000 Group Policy**	**V1.1**	13/11/2001	02
	I	**Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool**	**V1.1**	22/01/2002	03
	P	**Guide to Securing Microsoft Windows 2000 File and Disk Resources**	**V1.0**	19/04/2001	08
	P	**Guide to Securing Microsoft Windows 2000 DNS**	**V1.0**	09/04/2001	06
	P	**Guide to Securing Microsoft Windows 2000 Encrypting File System**	**V1.0**	01/01/2001	07
	P	**Guide to Windows 2000 Kerberos Settings**	**V1.1**	27/06/2001	16
	P	**Microsoft Windows 2000 Router Configuration Guide**	**V1.02**	01/05/2001	17
	R	**Guide to Securing Windows NT/9x Clients in a Windows 2000 Network**	**V1.03**	06/03/2002	10

Annuaire

	I	**Guide to Securing Microsoft Windows 2000 Schema**	**V1.0**	06/03/2001	09
	I	**Guide to Securing Microsoft Windows 2000 Active Directory**	**V1.0**	01/12/2000	05

Certificats

	R	**Guide to the Secure Config. & Admin. of Microsoft W2K Certificate Services**	**V2.11**	10/10/2001	12
	R	**Guide to the Secure Config. & Admin. of Microsoft W2K Certificate Services (check)**	**V2.02**	10/10/2001	13
	R	**Guide to Using DoD PKI Certificates in Outlook 2000**	**V3.1**	08/04/2002	15

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Services annexes					
	I	Guide to Secure Configuration & Administration of Microsoft ISA Server 2000	V1.41	07/01/2002	11
	P	Guide to the Secure Configuration & Administration of Microsoft IIS 5.0	V1.31	04/03/2002	14
	P	Guide to Securing Microsoft Windows 2000 DHCP	V1.2	25/06/2001	18
	P	Guide to Securing Microsoft Windows 2000 Terminal Services	V1.0	02/07/2001	19
	P	Microsoft Windows 2000 IPsec Guide	V1.0	13/08/2001	20
	P	Guide to the Secure Configuration and Administration of Microsoft Exchange 2000	V1.1	12/04/2002	21
Windows NT					
	P	Guide to Securing Microsoft Windows NT Networks	V4.2	18/09/2001	nt1
Cisco					
	R	Router Security Configuration Guide, Executive Summary	V1.0c	27/12/2001	cis1
✓	P	Router Security Configuration Guide	V1.1	27/09/2002	cis2
Contenus exécutables					
	R	E-mail Security in the Wake of Recent Malicious Code Incidents	V2.5	20/08/2001	eec1
	P	Guide to the Secure Configuration and Administration of Microsoft Exchange 5	V3.0	07/01/2002	eec2
	R	Microsoft Office 97 Executable Content Security Risks and Countermeasures	V1.1	20/12/1999	eec3
	R	Microsoft Office 2000 Executable Content Security Risks and Countermeasures	ND	08/02/2002	eec4
Documents de Support					
	I	Defense in Depth	ND	ND	sd01
	P	Guide to the Secure Configuration & Administration of iPlanet Web Serv Ent. Ed. 4.1	V1.73	03/07/2001	sd02
	P	Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0	V1.33	04/03/2002	sd03
	P	Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0 (Checklist Format)	V1.33	04/03/2002	sd04
	P	Secure Config. of the Apache Web Server, Apache Server V1.3.3 on Red Hat Linux 5.1	V1.12	24/04/2001	sd05
	R	Microsoft NetMeeting 3.0 Security Assessment and Configuration Guide	V1.14	05/10/2001	sd06
	R	The 60 Minute Network Security Guide	V1.1	18/02/2002	sd07
✎	R	Guide to Securing Microsoft Internet Explorer 5.5 Using Group Policy	V1.0	07/2002	sd08

Cette impressionnante liste de documents de sécurité mis à la disposition de tous par la **NSA** constitue un inestimable fond documentaire exploitable, sans grand travail d'adaptation, par les personnels ayant en charge la mise en place et la sécurisation d'architectures construites autour de produits **CISCO** et **Microsoft**.

- **Complément d'information**

http://nsa1.www.conxion.com/

LA LEGISLATION

USA

DECSS – LA COMPETENCE DES TRIBUNAUX CALIFORNIENS REJETEE

- **Description**

En décembre 1999, l'ampleur de l'affaire dite '**DeCSS**' défraie la chronique judiciaire : l'organisation **DVD CCA** – **DVD C**opy **C**ontrol **A**ssociation – attaque en justice des centaines d'individus et d'associations pour avoir développé et aidé à diffuser le programme gratuit '**DeCSS**' permettant de contourner le système de protection des supports **DVD** dit '**C**ontent **S**cambling **S**ystem'. L'histoire dit que le programme '**DeCSS**' aurait été développé dans l'optique de pouvoir disposer d'un logiciel de visualisation des DVD libre de tout droit en environnement LINUX. La seule certitude a ce sujet est que le code original a bien été posté en Octobre 1999 sur la liste du projet '**Livid**', un player multmédia.

En août 2001, une cour de justice de l'état de Californie rendait son jugement à l'encontre de **Matthew Povlovich** poursuivi pour avoir diffusé le code '**DeCSS**' sur le site WEB qu'il gérait depuis sa résidence au Texas. L'argument de l'accusé selon lequel il ne pouvait être jugé en Californie puisque ne résidant pas dans cet état n'avait pas été pris en compte à la grande satisfaction de l'accusation dont l'avocat annonçait à la presse:

"We're very pleased with the court's decision because it stands for the principle that individuals who steal trade secrets cannot hide behind the Internet as a shield to protect them from responsibility for their unlawful conduct,"

Un recours auprès de la Cour Suprême de Californie a alors été engagé par **Matthew Povlovich** avec l'aide de l'**EFF**, - **Electronic Frontier Foundation** – la célèbre association américaine indépendante qui milite pour le respect des droits et des libertés du citoyen dans l'espace de communication ouvert par les nouvelles technologies.

Le 25 novembre 2002, la Cour Suprême de Californie rendait son jugement en considérant que les tribunaux de l'Etat de Californie n'ont pas le pouvoir de juger quelqu'un résidant en dehors de leur domaine de juridiction, dans le cas présent, le territoire de l'état de Californie.

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

La Cour Suprême de Californie considère à ce propos qu'il est absolument nécessaire de disposer de règles légiférant la juridiction des tribunaux aux Etats-Unis, faute de quoi les poursuites liées à une industrie donnée seront engagées dans l'état où cette industrie est la plus florissante: Michigan pour l'automobile, Californie pour l'informatique, New York pour les technologies de la finance ou encore l'Idaho pour l'industrie de la pomme de terre ! Nous plaignons **Andrew Brunner**, le seul résidant Californien parmi l'ensemble des personnes citées à comparaître au titre de l'instruction engagée en décembre 1999.

On notera qu'une affaire similaire pourrait bien voir le jour dans les semaines à venir à la suite de la publication mi-décembre d'une implémentation de l'algorithme '**CSA**' (Common Scambling Algorithm) utilisé pour protéger les flux **DVB** (Digital Video Broadcast). Non public, cet algorithme a pu être reconstitué grâce aux informations contenues dans les brevets déposés par la société '**LSI Logic**' portant sur l'implémentation matérielle de l'algorithme !

En pratique, la diffusion à titre 'éducatif' du logiciel '**DeCSA**' ne devrait cependant pas mettre en péril la sécurité de l'infrastructure **DVB**, l'algorithme '**CSA**' utilisant un procédé de changement régulier de la clef dont la longueur de 64bits doit permettre d'assurer un niveau de sécurité correct … sauf à découvrir une faille majeure dans l'algorithme maintenant que celui-ci est connu.

- **Complément d'information**

http://www.dvdcca.org/
http://www.eff.org/IP/Video/DVDCCA_case/20021125_eff_pr.html
http://www.lemuria.org/DeCSS/decss.html
http://csa.irde.to/deCSA.html

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

LOGICIELS LIBRES

LES SERVICES DE BASE

Les dernières versions des services de base sont rappelées dans les tableaux suivants. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

RESEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.2.2rc1	14/08/02	http://www.isc.org/products/BIND
		8.3.4	16/11/02	
DHCP	Serveur d'adresse	3.0p1	08/05/02	http://www.isc.org/products/DHCP/dhcp-v3.html
NTP4	Serveur de temps	4.1.1b	26/10/02	http://www.eecis.udel.edu/~ntp
WU-FTP	Serveur de fichiers	2.6.2	29/11/01	http://www.wu-ftpd.org

MESSAGERIE

Nom	Fonction	Ver.	Date	Source
IMAP4	Relevé courrier	2002a	12/12/02	ftp://ftp.cac.washington.edu/imap/
POP3	Relevé courrier	4.0.4	12/04/02	ftp://ftp.qualcomm.com/eudora/servers/unix/popper/
SENDMAIL	Serveur de courrier	8.12.6	26/08/02	ftp://ftp.sendmail.org/pub/sendmail/RELEASE_NOTES

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.27	03/10/02	http://httpd.apache.org/dist
		2.0.43	03/10/02	
ModSSL	API SSL Apache 1.3.27	2.8.12	23/10/02	http://www.modssl.org
MySQL	Base SQL	3.23.55	11/12/02	http://www.mysql.com/doc/N/e/News-3.23.x.html
SQUID	Cache WEB	2.5s1	25/09/02	http://www.squid-cache.org

AUTRE

Nom	Fonction	Ver.	Date	Source
INN	Gestion des news	2.3.3	07/05/01	http://www.isc.org/products/INN
MAJORDOMO	Gestion des listes	1.94.5	15/01/00	http://www.greatcircle.com/majordomo
OpenCA	Gestion de certificats	0.9.02	13/09/02	http://www.openca.org/openca/download-releases.shtml
OpenLDAP	Gestion de l'annuaire	2.1.9	03/12/02	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/

LES OUTILS

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public est proposée dans les tableaux suivants.

LANGAGES

Nom	Fonction	Ver.	Date	Source
SPLINT	Analyse de code	3.0.1.6	18/02/02	http://lclint.cs.virginia.edu
Perl	Scripting	5.8.0	12/08/02	http://www.cpan.org/src/index.html
PHP	WEB Dynamique	4.2.3	06/09/02	http://www.php.net/downloads.php

ANALYSE RESEAU

Nom	Fonction	Ver.	Date	Source
Big Brother	Visualisateur snmp	1.9c	15/05/02	http://bb4.com/
Dsniff	Boite à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.6.7	02/07/02	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.9.8	09/12/02	http://www.ethereal.com
IP Traf	Statistiques IP	2.7.0	19/05/02	http://cebu.mozcom.com/riker/iptraf/
Nstreams	Générateur de règles	1.0.3	06/08/02	http://www.hsc.fr/ressources/outils/nstreams/download/
SamSpade	Boite à outils	1.14	10/12/99	**Erreur! Signet non défini.**
TcpDump	Analyse multiprotocole	3.7.1	21/01/02	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.7.1	21/01/02	http://www.tcpdump.org/
TcpFlow	Collecte données	0.20	26/02/01	http://www.circlemud.org/~jelson/software/tcpflow/
TcpShow	Collecte données	1.81	21/03/00	http://ftp7.usa.openbsd.org/pub/tools/unix/sysutils/tcpshow
WinPCap	Acquisition Trame	3.0alpha4	22/10/02	http://winpcap.polito.it/news.htm

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ANALYSE DE JOURNAUX

Nom	Fonction	Ver.	Date	Source
Analog	Journaux serveur http	5.30	30/11/02	http://www.analog.cx
Autobuse	Analyse syslog	1.13	31/01/00	http://www.picante.com/~gtaylor/autobuse
SnortSnarf	Analyse Snort	021111	02/11/02	**Erreur! Signet non défini.**
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SECURITE

Nom	Fonction	Ver.	Date	Source
FIRE	Boite à outils	0.3.5b	29/11/02	**Erreur! Signet non défini.**
curl	Analyse http et https	7.10.2	18/11/02	http://curl.haxx.se/
Nessus	Vulnérabilité réseau	1.2.7	17/12/02	http://www.nessus.org
Nmap	Vulnérabilité réseau	3.00	01/08/02	http://www.insecure.org/nmap/nmap_download.html
Pandora	Vulnérabilité Netware	4.0b2.1	12/02/99	http://www.packetfactory.net/projects/pandora/
Saint	Vulnérabilité réseau	4.1.3	13/12/02	http://www.saintcorporation.com/updates.html
Sara	Vulnérabilité réseau	4.1.2	05/11/02	http://www.www-arc.com/sara/downloads/
Tara (tiger)	Vulnérabilité système	3.0.3	15/08/02	http://www-arc.com/tara
Tiger	Vulnérabilité système	2.2.4p1	19/07/99	ftp://net.tamu.edu/pub/security/TAMU/tiger
Trinux	Boite à outils	0.81pre0	07/11/01	http://sourceforge.net/projects/trinux/
Whisker	Requêtes HTTP	2.1	29/11/02	http://www.wiretrip.net/rfp/p/doc.asp?id=21
	LibWhisker	1.6	29/11/02	

CONFIDENTIALITE

Nom	Fonction	Ver.	Date	Source
OpenPGP	Signature/Chiffrement			**Erreur! Signet non défini.**
GPG	Signature/Chiffrement	1.2.1	25/10/02	http://www.gnupg.org

CONTROLE D'ACCES

Nom	Fonction	Ver.	Date	Source
TCP Wrapper	Accès services TCP	7.6		ftp://ftp.cert.org/pub/tools/tcp_wrappers
Xinetd	Inetd amélioré	2.3.9	24/09/02	http://synack.net/xinetd/

CONTROLE D'INTEGRITE

Nom	Fonction	Ver.	Date	Source
Tripwire	Intégrité LINUX	2.3.47	15/08/00	http://www.tripwire.org/downloads/index.php
ChkRootKit	Compromission UNIX	0.38	20/09/02	http://www.chkrootkit.org/

DETECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
Deception TK	Pot de miel	19990818	18/08/99	http://all.net/dtk/index.html
LLNL NID	IDS Réseau	2.6	10/10/02	http://ciac.llnl.gov/cstc/nid/nid.html
Snort	IDS Réseau	1.9.0	03/10/02	http://www.snort.org/dl/
Shadow	IDS Réseau	1.7	21/09/01	http://www.nswc.navy.mil/ISSEC/CID/

GENERATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
Elza	Requêtes HTTP	1.4.5	01/04/00	http://www.stoev.org/elza/project-news.html
FireWalk	Analyse filtres	5.0	20/10/02	http://www.packetfactory.net/firewalk
IPSend	Paquets IP	2.1a	19/09/97	ftp://coombs.anu.edu.au/pub/net/misc
IDSWakeUp	Détection d'intrusion	1.0	13/10/00	http://www.hsc.fr/ressources/outils/idswakeup/download/
UdpProbe	Paquets UDP	1.2	13/02/96	http://sites.inka.de/sites/bigred/sw/udpprobe.txt

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBsd	3.1	19/04/00	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	3.4.31	07/12/02	http://coombs.anu.edu.au/ipfilter/ip-filter.html

TUNNELS

Nom	Fonction	Ver.	Date	Source
CIPE	Pile Crypto IP (CIPE)	1.5.4	29/06/01	http://sites.inka.de/sites/bigred/devel/cipe.html
FreeSwan	Pile IPSec	1.99	04/11/02	http://www.freeswan.org
http-tunnel	Encapsulation http	3.0.5	06/12/00	http://www.nocrew.org/software/httptunnel.html
		3.3 (dev)	08/03/01	
OpenSSL	Pile SSL	0.9.6g	06/12/02	http://www.openssl.org/
OpenSSH	Pile SSH 1 et 2	3.5	14/10/02	http://www.openssh.com/
Stunnel	Proxy https	4.03	27/10/02	http://www.stunnel.org
TTSSH	PlugIn SSH TeraTerm	1.54	21/03/01	http://www.zip.com.au/~roca/ttssh.html
Zebedee	Tunnel TCP/UDP	2.4.1	29/05/02	http://www.winton.org.uk/zebedee/

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

NORMES ET STANDARDS

LES PUBLICATIONS DE L'IETF

LES RFC

Du **23/11/2002** au **20/12/2002**, **33 RFC** ont été publiés dont 5 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
DNS	3445	12/02	Pst	Limiting the Scope of the KEY Resource Record (RR)
TLS	3436	12/02	Pst	Transport Layer Security over Stream Control Transmission Protocol
USM	3414	12/02	STD	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol

RFC TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Num	Date	Etat	Titre
SNMP	3415	12/02	STD	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

AUTRES RFC

Thème	Num	Date	Etat	Titre
CRANE	3423	11/02	Inf	XACCT's Common Reliable Accounting for Network Element (CRANE) Protocol Specification Version 1
DHCP	3442	12/02	Pst	The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4
IETF	3324	11/02	Inf	Short Term Requirements for Network Asserted Identity
	3410	12/02	Inf	Introduction and Applicability Statements for Internet-Standard Management Framework
	3419	12/02	Pst	Textual Conventions for Transport Addresses
	3432	11/02	Pst	Network performance measurement with periodic streams
	3439	12/02	Inf	Some Internet Architectural Guidelines and Philosophy
MAPOS	3422	11/02	Inf	Forwarding MAC Frames over MAPOS Optical Network/Synchronous Digital Hierarchy
MIB	3433	12/02	Pst	Entity Sensor Management Information Base
MIME	3391	12/02	Inf	The MIME Application/Vnd.pwg-multiplexed Content-Type
PPP	3336	12/02	Pst	PPP Over Asynchronous Transfer Mode Adaptation Layer 2 (AAL2)
	3337	12/02	Pst	Class Extensions for PPP over Asynchronous Transfer Mode Adaptation Layer 2
RTP	3409	12/02	Inf	Lower Layer Guidelines for Robust RTP/UDP/IP Header Compression
SDP	3388	12/02	Pst	Grouping of Media Lines in the Session Description Protocol (SDP)
SIEVE	3431	12/02	Pst	Sieve Extension: Relational Tests
SIP	3325	11/02	Inf	Private Extensions to SIP for Asserted Identity within Trusted Networks
	3326	12/02	Pst	The Reason Header Field for the Session Initiation Protocol (SIP)
	3327	12/02	Pst	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
	3427	12/02	BCP	Change Process for the Session Initiation Protocol (SIP)
	3428	12/02	Pst	Session Initiation Protocol (SIP) Extension for Instant Messaging
SLP	3421	11/02	Exp	Select and Sort Extensions for the Service Location Protocol (SLP)
SNMP	3411	12/02	STD	An Architecture for Describing SNMP Management Frameworks
	3412	12/02	STD	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
	3413	12/02	STD	Simple Network Management Protocol (SNMP) Applications
	3416	12/02	STD	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
	3417	12/02	STD	Transport Mappings for the Simple Network Management Protocol (SNMP)
	3418	12/02	STD	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
	3430	12/02	Exp	Simple Network Management Protocol Over Transmission Control Protocol Transport Mapping
TCP	3449	12/02	BCP	TCP Performance Implications of Network Path Asymmetry

LES DRAFTS

Du **23/11/2002**au **20/12/2002**, 228 drafts ont été publiés: **168** drafts mis à jour, **60** nouveaux drafts, dont **10** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-mun-aaa-dbu-mobileipv6-00	16/12	Dynamic Binding Update using AAA
DNS	draft-danisch-dns-rr-smtp-00	03/12	A DNS RR for simple SMTP sender authentication
HEALTH	draft-marshall-security-audit-00	02/12	Security Audit & Access Account. Msg Data Def. for Healthcare Ap.

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

IKE	draft-hoffman-sla-00	18/12	Secure Legacy Authentication (SLA) for IKEv2
IPV6	draft-bellovin-ipv6-accessprefix-00	25/11	Access Control Prefix Router Advertisement Option for IPv6
MSEC	draft-ietf-msec-ipsec-multicast-issues-00	06/12	IP Multicast issues with IPsec
RADIUS	draft-heinanen-radius-pe-discovery-00	18/12	Using Radius for PE-Based VPN Discovery
RSERP	draft-ietf-rserpool-threats-00	12/12	Threats Introduced by Rserpool & Reqs for Security in response to
SIP	draft-shenoy-sip-via-validation-00	18/12	SIP Ext. for Response Integrity Check using Validation Cookie
SRP	draft-papadimitratos-secure-rout-protocol-00	11/12	The Secure Routing Protocol (SRP) for Ad Hoc Networks

MISE A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-mun-aaa-localkm-mobileipv6-01	16/12	Localized Key Management for AAA in Mobile IPv6
BGP	draft-lonvick-sobgp-radius-01	09/12	RADIUS Attributes for soBGP Support
BMWG	draft-ietf-bmwg-firewall-07	16/12	Benchmarking Methodology for Firewall Performance
BTSH	draft-gill-btsh-01	09/12	The BGP TTL Security Hack (BTSH)
CRYPT	draft-leech-chinese-lottery-01	26/11	Chinese Lottery Cryptanalysis Revisited
DNS	draft-ietf-dnsext-keyrr-key-signing-flag-04	03/12	KEY RR Key-Signing Key (KSK) Flag
EAP	draft-puthenkulam-eap-binding-01	03/12	The Compound Authentication Binding Problem
IDMEF	draft-ietf-idwg-idmef-xml-09	02/12	Intrusion Detection Message Exch Format Data Model & XML DTD
IP	draft-ietf-ips-auth-mib-03	06/12	Definitions of Managed Objects for User Identity Authentication
IP	draft-ietf-ips-security-18	11/12	Securing Block Storage Protocols over IP
IPSEC	draft-ietf-ipsp-ipsec-conf-mib-05	11/12	IPsec Policy Configuration MIB
	draft-ietf-ipsp-ipsecpib-06	11/12	IPSec Policy Information Base
IPV6	draft-savola-ipv6-rh-ha-security-03	02/12	Security of IPv6 Routing Header and Home Address Options
	draft-savola-v6ops-6to4-security-01	06/12	Security Considerations for 6to4
MOBILEIP	draft-ietf-mobileip-aaa-nai-03	27/11	AAA NAI for Mobile IPv4 Extension
	draft-tessier-mobileip-ipsec-01	02/12	Guidelines for Mobile IP and IPSec VPN Usage
PKIX	draft-ietf-pkix-certstore-http-03	18/12	X.509 PKI Operational Protocols: Certificate Store Access via HTTP
	draft-ietf-pkix-ocspv2-ext-01	12/12	X.509 Internet PKI Online Certificate Status Protocol, version 2
	draft-ietf-pkix-pi-06	04/12	X.509 PKI Permanent Identifier
	draft-ietf-pkix-rfc2510bis-07	27/11	X.509 PKI Certificate Management Protocols
	draft-ietf-pkix-rfc2511bis-05	27/11	X.509 PKI Certificate Request Message Format (CRMF)
	draft-ietf-pkix-wlan-extns-04	16/12	Certificate Ext and Attributes Supporting Auth. in PPP and WiFi
PPP	draft-aboba-pppext-key-problem-04	11/12	EAP Key Management Guidelines
	draft-ietf-pppext-rfc2284bis-08	03/12	Extensible Authentication Protocol (EAP)
RADIUS	draft-aboba-radius-rfc2869bis-05	16/12	RADIUS Support For Extensible Authentication Protocol (EAP)
SILC	draft-riikonen-silc-ke-auth-06	26/11	SILC Key Exchange and Authentication Protocols
	draft-riikonen-silc-spec-06	27/11	Secure Internet Live Conferencing (SILC), Protocol Specification
SMIME	draft-ietf-smime-symkeydist-08	16/12	CMS Symmetric Key Management and Distribution
SYSLOG	draft-ietf-syslog-sign-08	16/12	Syslog-Sign Protocol
TLS	draft-ietf-tls-compression-04	02/12	Transport Layer Security Protocol Compression Methods
	draft-ietf-tls-srp-04	02/12	Using SRP for TLS Authentication

DRAFTS TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-aaa-diameter-16	18/12	Diameter Base Protocol
	draft-ietf-aaa-diameter-nasreq-10	02/12	Diameter NASREQ Application
	draft-loughney-aaa-cc-3gpp-01	04/12	Diameter Command Codes for 3GPP Release 5
BMWG	draft-ietf-bmwg-mcastm-10	02/12	Methodology for IP Multicast Benchmarking
ECML	draft-ietf-trade-ecml2-spec-06	26/11	ECML:Version 2 Specification
IDWG	draft-ietf-idwg-beep-tunnel-05	06/12	The TUNNEL Profile
ISATAP	draft-ietf-ngtrans-isatap-07	16/12	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
LDAP	draft-ietf-ldapbis-models-06	16/12	LDAP: Directory Information Models
	draft-ietf-ldapbis-protocol-12	03/12	LDAP: The Protocol
	draft-joslin-config-schema-05	02/12	A Configuration Schema for LDAP Based Directory User Agents
	draft-zeilenga-ldapbis-rfc2253-02	16/12	LDAP: String Representation of Distinguished Names
	draft-zeilenga-ldap-rfc2596-04	11/12	Language Tags and Ranges in LDAP
	draft-zeilenga-ldapv2-04	18/12	LDAPv2 to Historical Status
LSB	draft-bartz-lsb-policy-rule-components-00	09/12	Logically Succinct Basic Policy Rule Components
POLICY	draft-reyes-policy-core-ext-schema-00	18/12	Policy Core Extension LDAP Schema (PCELS)
VPN	draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-02	18/12	Generalized Provider-prov. Port-based VPNs using BGP & GMPLS

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-aaa-transport-09	09/12	AAA Transport Profile
ACAP	draft-ietf-acap-abook-03	27/11	ACAP Personal Addressbook Dataset Class
	draft-ietf-acap-option-05	02/12	ACAP Application Options Dataset Class
ALGO	draft-misbahuddin-data-reduc-00	02/12	Dev. of an Algorithm to Reduce Internet Data Traffic Congestion
ATOMMIB	draft-ietf-atommib-opticalmib-07	11/12	Definitions of Managed Objects for the Optical Interface Type
AUTO	draft-white-auto-subnet-00	09/12	Automatic Globally Unique Site Local Subnet Allocation
AVT	draft-ietf-avt-mpeg4-simple-05	11/12	Transport of MPEG-4 Elementary Streams
BGP	draft-chen-bgp-prefix-orf-05	16/12	Address Prefix Based Outbound Route Filter for BGP-4
	draft-ietf-idr-as4bytes-06	16/12	BGP support for four-octet AS number space

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	draft-ietf-idr-aspath-orf-04	04/12	Aspath Based Outbound Route Filter for BGP-4
	draft-ietf-idr-bgp-gr-survey-00	06/12	BGP Graceful Restart - Implementation Survey
	draft-ietf-idr-cease-subcode-02	25/11	Subcodes for BGP Cease Notification Message
	draft-ietf-idr-dynamic-cap-03	26/11	Dynamic Capability for BGP-4
	draft-ietf-idr-route-filter-07	02/12	Cooperative Route Filtering Capability for BGP-4
BIP	draft-prasanna-bip-00	16/12	BIP: Billing Information Protocol
BRIDGE	draft-ietf-bridge-bridgemib-smiv2-04	09/12	Definitions of Managed Objects for Bridges
CN	draft-ietf-cdi-known-request-routing-02	06/12	Known CN Request-Routing Mechanisms
DDP	draft-ietf-rddp-arch-00	12/12	The Architecture of DDP And RDMA On Internet Protocols
	draft-ietf-rddp-problem-statement-00	12/12	RDMA over IP Problem Statement
	draft-ietf-rddp-rdma-concerns-00	02/12	DDP and RDMA Concerns
	draft-stewart-rddp-sctp-01	12/12	SCTP RDMA Direct Data Placement (DDP) Adaption
DHCP	draft-ietf-dhc-dhcpv6-opt-prefix-delegation-01	02/12	IPv6 Prefix Options for DHCPv6
	draft-ietf-dhc-isnsoption-04	18/12	DHCP Options for Internet Storage Name Service
	draft-ietf-ipoib-dhcp-over-infiniband-03	27/11	DHCP over InfiniBand
DNS	draft-bhatla-dnsext-murr-00	16/12	DNS RR type for Multiple Unicast
	draft-ietf-dnsext-axfr-clarify-05	02/12	DNS Zone Transfer Protocol Clarifications
	draft-ietf-dnsext-delegation-signer-12	04/12	Delegation Signer Resource Record
	draft-ietf-dnsext-ipv6-name-auto-reg-00	11/12	Domain Name Auto-Registration for Plugged-in IPv6 Nodes
	draft-ietf-dnsext-mdns-13	03/12	Linklocal Multicast Name Resolution (LLMNR)
	draft-xdlee-cnamestr-01	25/11	Chinese Name String in Search-based access model for the DNS
EAPS	draft-shah-extreme-eaps-00	18/12	Ethernet Automatic Protection Switching (EAPS), Version 1
ENUM	draft-ietf-enum-rfc2916bis-02	25/11	The E.164 to URI DDDS Application (ENUM)
ETS	draft-carlberg-ets-general-01	06/12	General Requirements for Emergency Telecommunication Service
	draft-carlberg-ets-telephony-01	06/12	IP Telephony reqs for Emergency Telecommunication Service
FORCES	draft-ietf-forces-applicability-01	16/12	ForCES Applicability Statement
	draft-ietf-forces-netlink-04	16/12	Netlink as an IP Services Protocol
GEOPRIV	draft-schulzrinne-geopriv-dhcp-civil-00	06/12	DHCP Option for Civil Location
H248	draft-rogupta-hss-megaco-legal-intercept-00	11/12	Legal Intercept Package for Megaco/H.248
HANDLE	draft-sun-handle-system-def-07	27/11	Handle System Namespace and Service Definition
	draft-sun-handle-system-protocol-04	27/11	Handle System Protocol (ver 2.1) Specification
I18N	draft-hoffman-i18n-terms-11	03/12	Terminology Used in Internationalization in the IETF
IANA	draft-iab-iana-00	16/12	Defining the Role and Function of the IETF-IANA
IEPREP	draft-polk-ieprep-scenarios-02	03/12	IEPREP Topology Scenarios
IESG	draft-iesg-charter-00	06/12	An IESG charter
	draft-klensin-overload-00	11/12	IESG Overload and Quantity of WGs
IETF	draft-blanchet-evolutionizeietf-suggestions-00	27/11	Suggestions to Streamline the IETF Process
iFCP	draft-ietf-ips-ifcp-14	04/12	iFCP - A Protocol for Internet Fibre Channel Storage Networking
IKEV2	draft-dukes-ikev2-config-payload-00	18/12	Configuration payload
IMAP	draft-ietf-imapext-sort-11	16/12	IMAP - SORT AND THREAD EXTENSION
IMAP	draft-melnikov-imap-mdn-05	03/12	MDN profile for IMAP
IMPP	draft-ietf-impp-im-01	06/12	Common Profile: Instant Messaging
	draft-ietf-impp-pres-01	06/12	Common Profile: Presence
	draft-ietf-impp-srv-01	06/12	Address Resolution for Instant Messaging and Presence
IP	draft-boucadair-ipte-acct-pib-01	06/12	An IP Traffic Engineering PIB for Accounting purposes
	draft-cheshire-ipv4-acd-03	11/12	IPv4 Address Conflict Detection
	draft-dreibholz-ipv4-flowlabel-01	02/12	An IPv4 Flowlabel Option
IPO	draft-ietf-iporpr-core-00	06/12	A Core Standard For Transmission of IP Packets Over IEEE 802.17
IPSEC	draft-moon-ipsec-ipconc-00	09/12	The Concatenation of IP Packets
IPV6	draft-gopinath-ipv6-hostname-auto-reg-02	03/12	IPv6 Hostname auto-registration Procedure
	draft-hinden-ipv6-global-site-local-00	06/12	IPv6 Globally Unique Site-Local Addresses
	draft-ietf-ipngwg-rfc2553bis-10	18/12	Basic Socket Interface Extensions for IPv6
	draft-ietf-ipv6-flow-label-04	18/12	IPv6 Flow Label Specification
	draft-ietf-v6ops-3gpp-analysis-00	09/12	Analysis on IPv6 Transition in 3GPP Networks
	draft-ietf-vrrp-ipv6-spec-03	06/12	Virtual Router Redundancy Protocol for IPv6
	draft-moore-ipv6-optimistic-dad-01	25/11	Optimistic Duplicate Address Detection
	draft-pouffary-v6ops-ent-v6net-02	11/12	IPv6 Enterprise Networks Scenarios
	draft-soohong-ipv6-deployment-00	18/12	IPv6 Deployment using Device ID
	draft-wasserman-ipv6-sl-impact-00	18/12	The Impact of Site-Local Addressing in IPv6
IRC	draft-brocklesby-irc-isupport-01	09/12	IRC RPL_ISUPPORT Numeric Definition
	draft-brocklesby-irc-usercmdpfx-02	09/12	IRC Command Prefix Capability
iSCSI	draft-ietf-ips-iscsi-boot-08	26/11	Bootstrapping Clients using the iSCSI Protocol
	draft-ietf-ips-iscsi-mib-08	06/12	Definitions of Managed Objects for iSCSI
ISIS	draft-ietf-isis-gmpls-extensions-15	06/12	IS-IS Extensions in Support of Generalized MPLS
	draft-ietf-isis-ipv6-04	02/12	Routing IPv6 with IS-IS
	draft-ietf-isis-traffic-04	18/12	IS-IS extensions for Traffic Engineering
iSNS	draft-ietf-ips-isns-15	11/12	Internet Storage Name Service (iSNS)
	draft-ietf-ips-isns-mib-03	16/12	Definitions of Managed Objects for iSNS
IUA	draft-bhola-conformance-test-iua-01	18/12	Conformance Test Specification for IUA
L2TP	draft-luo-l2tpext-l2vpn-signaling-00	27/11	L2VPN Signaling Using L2TPv3
LAP	draft-weijing-lap-ops-use-01	25/11	User Cases of Network Operation of Large Access Providers
LDP	draft-aboulmagd-ccamp-crldp-ason-ext-02	06/12	CR-LDP Extensions for ASON
LMP	draft-lang-ccamp-lmp-bootstrap-02	12/12	Control Channel Bootstrap for Link Management Protocol
MAGMA	draft-ietf-magma-mld-source-04	16/12	Source Address Selection for Multicast Listener Discovery Protocol
MAILLIS	draft-palme-maillist-02	02/12	Appropriate Mailing List Behaviour
MGCP	draft-foster-mgcp-bulkaudits-06	02/12	MGCP Bulk Audits Package
	draft-foster-mgcp-lockstep-00	02/12	MGCP Lockstep State Reporting Mechanism

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	draft-foster-mgcp-redirect-01	02/12	MGCP Redirect and Reset Package
MIB	draft-ietf-hubmib-wis-mib-05	16/12	Definition of MO for the Ethernet WAN Interface Sublayer
MLD	draft-vida-mld-v2-06	02/12	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
MO	draft-glenn-mo-aggr-mib-02	16/12	The Managed Object Aggregation MIB
	draft-glenn-mo-taggr-mib-01	16/12	The Aggregation MIB for time based samples of a Managed Object
MOBILEIP	draft-gwon-mobileip-efwd-fmipv6-00	18/12	eFWD From Prev Care-of Address For Fast Mobile IPv6 Handovers
	draft-ietf-mobileip-rfc3012bis-04	16/12	Mobile IPv4 Challenge/Response Extensions (revised)
MPLS	draft-andersson-mpls-sig-decision-03	27/11	The MPLS Working Group decision on MPLS signaling protocols
	draft-cetin-mpls-diffserv-te-mib-00	25/11	MPLS)Traffic Engineering MIB for DiffServ
	draft-ietf-mpls-crldp-unnum-10	27/11	Signalling Unnumbered Links in CR-LDP
	draft-ietf-mpls-lsp-query-05	06/12	MPLS Label Distribution Protocol Query Message Description
	draft-ietf-mpls-ttl-04	02/12	Time to Live (TTL) Processing in MPLS Networks (RFC 3032)
	draft-nadeau-mpls-dste-mib-00	16/12	Diff-Serv-aware MPLS Traffic Engineering Network MIB SMIv2
	draft-rabbat-fault-notification-protocol-01	02/12	Fault Notification Protocol for GMPLS-Based Recovery
	draft-ramalho-rgl-rtpformat-00	06/12	MPLS Inter-AS Traffic Engineering requirements
	draft-vijay-mpls-crldp-fastreroute-02	06/12	Fast Reroute Extensions to Constraint based Routed LDP
	draft-vijay-mpls-rsvpte-lspsubobject-01	02/12	LSP Subobject for RSVP-TE
	draft-zhang-mpls-interas-te-req-01	18/12	MPLS Inter-AS Traffic Engineering requirements
MSEC	draft-ietf-msec-gdoi-07	16/12	The Group Domain of Interpretation
MSGHEAD	draft-newman-msgheader-originfo-05	28/05	Originator-Info Message Header
NSIS	draft-ietf-nsis-req-06	18/12	Requirements for Signaling Protocols
NSRG	draft-irtf-nsrg-report-08	12/12	What's In A Name:Thoughts from the NSRG
NTLP	draft-brunner-nsis-ntlp-func-00	16/12	NSIS Transport Layer Protocol (NTLP) Functionality
OGG	draft-pfeiffer-ogg-fileformat-00	06/12	The Ogg encapsulation format version 0
	draft-walleij-ogg-mediatype-07	06/12	The application/ogg Media Type
OPES	draft-ietf-opes-architecture-04	12/12	An Architecture for Open Pluggable Edge Services (OPES)
	draft-ietf-opes-protocol-reqs-03	12/12	Requirements for OPES Callout Protocols
OSPF	draft-ietf-ccamp-ospf-gmpls-extensions-09	03/12	OSPF Extensions in Support of Generalized MPLS
	draft-ietf-ospf-hitless-restart-04	09/12	Hitless OSPF Restart
	draft-ietf-ospf-ospfv3-auth-00	09/12	Authentication/Confidentiality for OSPFv3
	draft-srisuresh-ospf-te-04	09/12	An experimental extension to OSPF for Traffic Engineering
PFL	draft-myers-pfl-04	02/12	Procedural Footnote Language Version 1.0
PIM	draft-ietf-pim-sm-v2-new-06	11/12	PIM - Sparse Mode PIM-SM): Protocol Specification (Revised)
PPP	draft-gpaterno-wireless-pppoe-06	06/12	Using PPP-over-Ethernet (PPPoE) to authenticate Wireless LANs
PRESENC	draft-riikonen-presence-attrs-01	26/11	User Online Presence and Information Attributes
PWE3	draft-ietf-pwe3-requirements-04	09/12	Requirements for Pseudo Wire Emulation Edge-to-Edge (PWE3)
	draft-riegel-pwe3-tdm-requirements-01	18/12	Reqs for Edge-to-Edge Emulation of TDM Circuits over PSN
QOS	draft-bianchi-qos-multicast-over-diffserv-00	02/12	MultiGRIP: Quality of Service Aware Multicasting over DiffServ
RFC2806	draft-antti-rfc2806bis-07	06/12	The tel URI for Telephone Calls
RGL	draft-ramalho-rgl-desc-00	06/12	RGL Codec Description Document
RMT	draft-ietf-rmt-bb-track-02	27/11	Reliable Multicast Transport Building Block for TRACK
	draft-ietf-rmt-bb-webrc-04	11/12	Wave and Equation Based Rate Control building block
ROHC	draft-hwang-rohc-mipv6-00	02/12	ROHC: A Compression Profile for Mobile IPv6
	draft-ietf-rohc-mib-rtp-05	16/12	Definitions of Managed Objects for Robus Header Compression
	draft-ietf-rohc-terminology-and-examples-01	03/12	ROHC:Terminology & Examples for MIB Modules & Channel Mapp.
RPS	draft-damas-rpslng-00	18/12	RPSLng
RTP	draft-banerjee-rtp-vod-00	26/11	Ext. of RTP and RTCP protocols For Video-on-Demand systems
	draft-ietf-avt-rfc2833bis-02	06/12	RTP Payload for DTMF Digits, Telephony Tones, Telephony Signals
	draft-ietf-avt-rtp-retransmission-04	18/12	RTP Retransmission Payload Format
	draft-ietf-avt-smpte292-video-08	03/12	RTP Payload Format for SMPTE 292M Video
	draft-xie-avt-dsr-es202050-00	12/12	RTP Payload Fmt for ETSI ES 202 050 Dist. Speech Recog. Encod
SEAMOBY	draft-nakhjiri-seamoby-ppp-ct-00	02/12	Enhanced PPP link re-establishment using context transfer
SHARED	draft-moskowitz-shared-secret-provprot-00	18/12	Shared Secret Provisioning Protocol
SIGTRAN	draft-ietf-sigtran-gr303ua-00	12/12	GR-303 extensions to the IUA protocol
SILC	draft-riikonen-flags-payloads-02	09/12	SILC Message Flag Payloads
	draft-riikonen-silc-commands-04	26/11	SILC Commands
	draft-riikonen-silc-pp-06	27/11	SILC Packet Protocol
SIP	draft-camarillo-sipping-early-media-00	02/12	Early Media and Ringback Tone Generation in SIP
	draft-ietf-ieprep-sip-reqs-03	06/12	Reqs for Resource Priority Mechanisms for SIP
	draft-ietf-simple-presence-09	06/12	A Presence Event Package for the Session Initiation Protocol (SIP)
	draft-ietf-sip-refer-07	04/12	The SIP Refer Method
	draft-rosenberg-simple-messaging-req-00	18/12	Advanced Instant Messaging Requirements for SIP
	draft-schulzrinne-sipping-sos-03	06/12	Emergency Services for Internet Telephony based on SIP
	draft-sinnreich-sipdev-req-00	02/12	SIP Telephony Device Requirements, Configuration and Data
SMIME	draft-ietf-smime-cms-rsaes-oaep-07	03/12	Use of the RSAES-OAEP Transport Algorithm in CMS
SNMP	draft-ietf-snmpv3-coex-v2-02	16/12	Coexistence of V1, V2, V3 of the Internet-standard NMF
SPEECHS	draft-ietf-speechsc-reqts-03	06/12	Reqs for Distributed Control of ASR, SI/SV and TTS Resources
TCP	draft-ietf-pilc-2.5g3g-12	09/12	TCP over 2.5G and 3G Generation Wireless Networks
	draft-ietf-tsvwg-tcp-eifel-alg-07	06/12	The Eifel Detection Algorithm for TCP
	draft-ietf-tsvwg-tcp-eifel-response-02	09/12	The Eifel Response Algorithm for TCP
	draft-ietf-tsvwg-udp-lite-01	06/12	The UDP-Lite Protocol
TEWG	draft-liljenstolpe-tewg-cwbcp-02	11/12	Offline Traffic Engineering in a Large ISP Setting
TRADE	draft-ietf-trade-voucher-lang-04	16/12	XML Voucher: Generic Voucher Language
UDP	draft-ietf-midcom-stun-04	11/12	Simple Traversal of UDP Through Network Address Translators
VPN	draft-ouldbrahim-ppvpn-gid-02	18/12	Global Unique Identifiers (GID)
	draft-ouldbrahim-ppvpn-ovpn-req-01	18/12	Service Requirements for Optical Virtual Private Networks
	draft-ouldbrahim-ppvpn-vpoxc-02	18/12	Provider Prov. GMPLS-based Virtual Private Cross-Connect Service

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	draft-raggarwa-ppvpn-mpls-ip-gre-sig-00	02/12	Signaling MPLS in IP or MPLS in GRE Encapsulation Capability
	draft-sodder-ppvpn-vhls-01	27/11	Virtual Hierarchical LAN Services
WEBDAV	draft-reschke-webdav-search-02	25/11	WebDAV SEARCH
WINFO	draft-ietf-simple-winfo-format-03	04/12	An XML Based Format for Watcher Information
	draft-ietf-simple-winfo-package-04	06/12	A Watcher Information Event Template-Package for SIP
XMPP	draft-ietf-xmpp-core-00	09/12	XMPP Core
	draft-ietf-xmpp-im-00	09/12	XMPP Instant Messaging
ZEROUTE	draft-linton-zerouter-requirements-00	16/12	Zerouter Protocol Requirements

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

NOS COMMENTAIRES

LES RFC

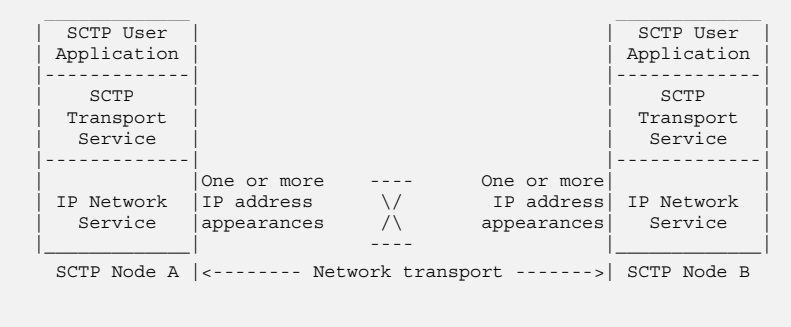
RFC3436

Transport Layer Security over Stream Control Transmission Protocol

Cette proposition de standard de 9 pages concerne l'utilisation du protocole de sécurité '**TLS**' (appellation **IETF** du protocole **SSLv3**) sur le protocole '**SCTP**'.

Spécifié par les **RFC 2960** et **RFC 3309**, le protocole '**SCTP**' a été étudié pour offrir un mécanisme fiable permettant de transporter les messages de signalisation d'un réseau commuté de téléphonie sur un réseau paquet tel que le réseau **IP**.

Le lecteur intéressé par l'implémentation et les applications pratiques de ce protocole pourra se reporter à l'excellente présentation '**SCTP for beginners**' proposée par l'université d'Essen.



'**SCTP**' offre entre autres fonctionnalités :

- Le transport fiable et la délivrance de messages dont l'intégrité est garantie,
- La fragmentation des messages en conformité avec la taille maximale d'un paquet sur le réseau,
- Le séquencement des messages dans les multiples flux avec la possibilité de délivrer ceux-ci dans l'ordre d'arrivée pour un utilisateur donné,
- La gestion des problèmes réseaux par le biais du support de multiples points d'accès – multihoming - de part et d'autre d'une association '**SCTP**'.

Spécifié par le **RFC2246**, le protocole '**TLS**' est conçu pour offrir un service de sécurité sur un transport de type 'flux d'octets' pour lequel il permettra d'établir l'authentification des deux extrémités et la confidentialité de l'échange. Son utilisation sur le protocole '**SCTP**' devra tenir compte des deux grandes spécificités de celui-ci:

- Flux de données multiples
- Protocole de transfert de messages

Le **RFC3436** détaille les différentes contraintes d'intégration en précisant les choix d'implémentation:

- Utilisation de l'option '**SCTP**' autorisant la gestion de la fragmentation des messages afin de garantir le transport d'un enregistrement '**TLS**' dans un message '**SCTP**', la taille maximal de celui-ci étant alors réduite à 18437 octets,
- Etablissement des sessions '**TLS**' sur les flux '**SCTP**' bidirectionnels, la négociation pouvant être gérée flux par flux ou sur la base la négociation du tout premier flux.

On notera la problématique mise en évidence dans le chapitre '**Security Consideration**' portant sur l'impact de la nature 'multipoints d'accès' du protocole '**SCTP**' : les enregistrements '**TLS**' émis par une entité authentifiée pourront provenir d'adresses IP autres que celle originellement authentifiée.

ftp://ftp.isi.edu/in-notes/rfc3436.txt

ftp://ftp.isi.edu/in-notes/rfc3309.txt

http://tdrwww.exp-math.uni-essen.de/inhalt/forschung/sctp_fb/

LES DRAFTS

DRAFT-IETF-INCH-IODEF-00

Incident Object Description and Exchange Format Data Model and XML DTD

Financé par l'association **TERENA** (**T**rans-**E**uropean **R**esearch **E**ducation **N**etworking **A**ssociation), le comité **TF-CSIRT** a pour mission de promouvoir la collaboration entre les **CSIRT** (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam). Ce comité a notamment œuvré pour disposer d'un modèle de représentation d'un incident de sécurité adapté au besoin des '**CSIRT**' (Rapports N°32 – Mars 2001 et N°46 – Mai 2002).

Les résultats des travaux, initialement engagés dans le cadre d'un groupe de travail interne dit '**IODEF WG**', ont été repris fin 2002 au sein du groupe '**INCH**' – **Extended Incident Handling** - de l'**IETF**.

Le calendrier des actions annoncées par ce groupe de travail est le suivant :

Septembre 2002	Premier ID (Internet Draft) portant sur les règles d'implémentation et des exemples
Décembre 2002	Premier ID (Internet Draft) de spécification des besoins et des exigences
	Soumission du document de spécification des besoins à l'**IESG** au titre 'Informel'

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

	Soumission du document de spécification du langage de description au titre de 'Proposition'
Janvier 2003	Soumission du document d'implémentation à l'**IESG** au titre 'Informel'

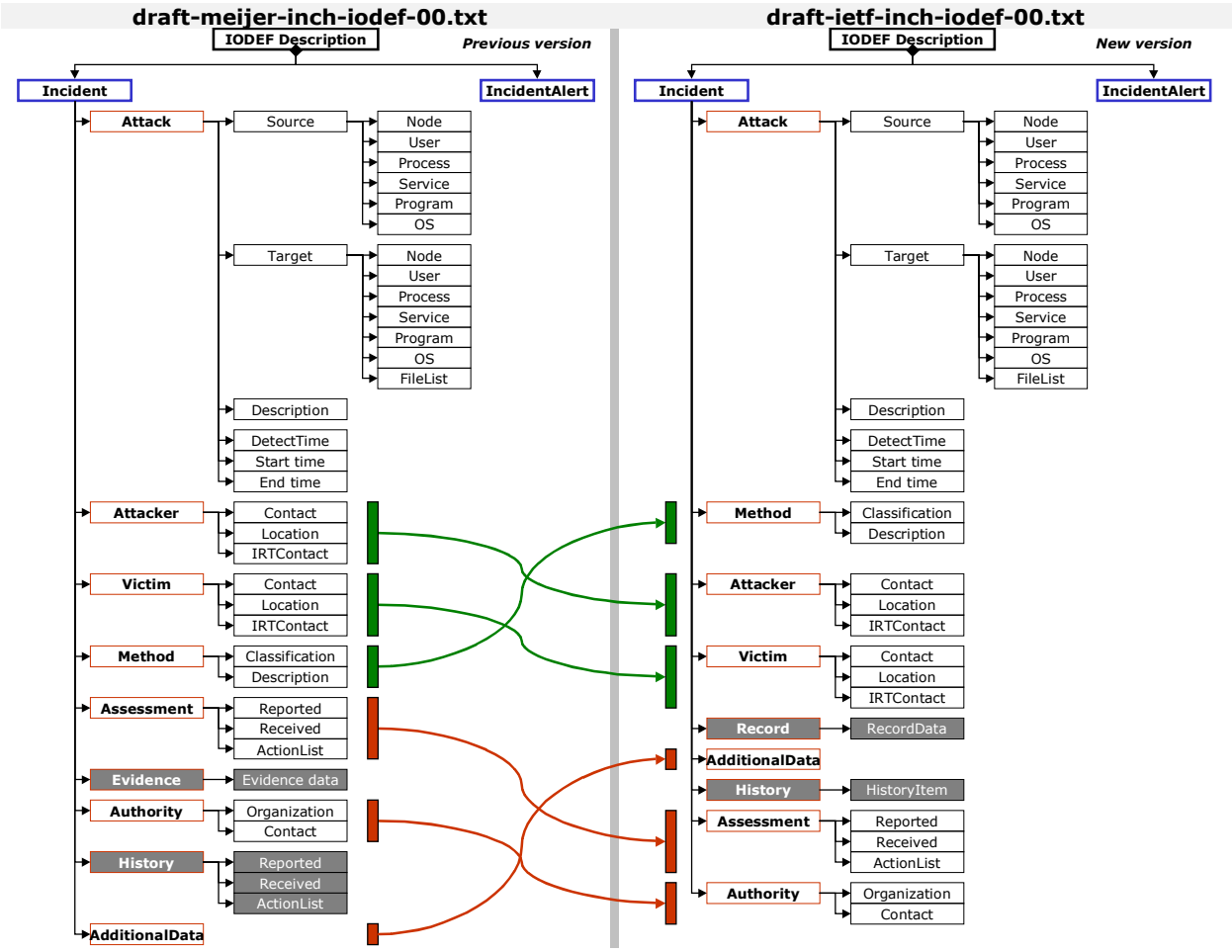
Le lecteur intéressé par les actions menées au sein de ce groupe de travail pourra consulter sa charte de fonctionnement disponible sur le site de l'**IETF**.

Initialement diffusé sous l'égide du groupe de travail '**IODEF**', le document intitulé '**Incident Object Description and Exchange Format Data Model and XML DTD**' a fait l'objet d'un première publication en avril 2002 dans le cadre de l'IETF sous la référence '**draft-meijer-inch-iodef-00.txt**' et pour une durée de validité de 6 mois. Objet de diverses modifications, ce document est désormais diffusé sous la référence '**draft-ietf-inch-iodef-00.txt**'.

Etant donnée l'importance du modèle de données spécifié par ce document, nous ne pouvons que déplorer l'absence d'une liste détaillant les modifications apportées entre les deux versions, et, ce d'autant que la date de publication n'a pas été changée dans les en-têtes de pages. Il est ainsi impossible de déterminer l'ampleur réelle des évolutions sans avoir à comparer chapitre par chapitre les 115 pages que comporte cette dernière version (contre 128 pages pour la version précédente).

Globalement – nous n'avons pas engagé de démarche de comparaison détaillée – les évolutions majeures sont principalement d'ordre 'cosmétique' : tournure de phrases, ré-ordonnancement de la présentation de certains objets, simplification de certains chapitres dont le chapitre 3.2 «**XML Document Type Definition**» expurgé des définitions élémentaires.

On notera cependant une évolution mineure du modèle de donnée. Le lecteur pourra s'en rendre compte en étudiant la présentation synthétique de chacune des deux versions ci-après :



En faisant abstraction du changement de l'ordonnancement de la présentation de certaines structures – la méthode prévaut désormais sur l'attaquant ou la victime du moins sur le plan de la stricte forme – seules deux modifications sont à noter :

- Simplification de la classe '**History**' initialement constituée de l'agrégation de trois classes et désormais réduite à la plus simple expression,
- Utilisation de la sémantique '**Record**' ('Enregistrement') en lieu et place de la sémantique '**Evidence**' ('Preuve'), cette dernière définition étant probablement trop ciblée.

On notera par ailleurs la spécification de la classe '**IRTContact**' permettant de définir un pointeur vers un annuaire public (telle la base '**whois**' maintenue par le **RIPE**) référençant les coordonnées des services chargés de gérer les incidents (CSIRT ou NOC) dans le contexte associé : renseignements concernant la victime (classe 'Victim') ou l'attaquant supposé (classe 'Attacker'). Ce pointeur pourra notamment référencer le champ '**IRT**' désormais géré - mais pas obligatoirement renseigné – dans les bases '**WhoIs**'.

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

La table des matières de cette nouvelle mouture est la suivante:

1. **Conventions Used in This Document**
2. **Introduction**
   2.1 IODEF Data MOdel Design principles
   2.1.1 Problems Addressed by the Data Mode
   2.1.2 Data Model Design Goals
   2.2 Using XML for the IODEF
   2.3 Relation between IODEF and IDMEF
3. **Notational Conventions and Formatting Issues**
   3.1 UML Conventions used for Data Model Description
   3.1.1 Relationships
   3.1.2 Occurrence Indicators
   3.2 XML Document Type Definitions
   3.3 XML Documents
   3.3.1 The Document Prolog
   3.3.1.1 XML Declaration
   3.3.1.2 IODEF DTD Formal Public Identifier
   3.3.1.3 IODEF DTD Document Type Declaration
   3.3.2 Character Data Processing in XML and IODEF
   3.3.2.1 Character Entity References
   3.3.2.2 Character Code References
   3.3.2.3 White Space Processing
   3.3.3 Languages in XML and IODEF
   3.3.4 Inheritance and Aggregation
   3.4 IODEF Data Types
   3.4.1 Integers
   3.4.2 Real Numbers
   3.4.3 Characters and Strings
   3.4.4 Bytes
   3.4.5 Enumerated Types
   3.4.6 Date-Time Strings
   3.4.7 NTP Timestamps
   3.4.8 Port Lists
   3.4.9 Unique Identifiers
   3.4.10 Personal names
   3.4.11 Organization name
   3.4.12 Postal address
   3.4.13 Telephone and Fax numbers
4. **The IODEF Data Model and XML DTD**
   4.1 Data Model Overview
   4.2 The IODEF-Description Class
   4.3 The Incident Class
   4.4 The CorrelationIncident Class
   4.4.1 The EventList Class
   4.5 The IncidentAlert Class
   4.6 The Attack Class
   4.6.1 The Source Class
   4.6.2 The Node Class
   4.6.2.1 The Address Class
   4.6.2.2 The NodeRole Class
   4.6.3 The User Class
   4.6.3.1 The UserId Class
   4.6.4 The Process Class
   4.6.5 The Service Class
   4.6.5.1 The WebService Class
   4.6.5.2 The SNMPService Class
   4.6.6 The Target Class
   4.6.7 The FileList Class
   4.6.7.1 The File Class
   4.6.7.2 The FileAccess Class
   4.6.7.3 The Linkage Class
   4.6.7.4 The Inode Class
   4.6.8 The Description Class
   4.6.9 The DetectTime Class
   4.6.10 The StartTime Class
   4.6.10 The EndTime Class
   4.7 The Method Class
   4.7.1 The Classification Class
   4.8 The Attacker Class
   4.8.1 The Contact Class
   4.8.2 The IRTcontact Class
   4.9 The Victim Class
   4.10 The Record Class
   4.10.1 The RecordData Class
   4.10.2 The CorrRecord Class
   4.10.3 The RecordDesc Class
   4.10.4 The Analyzer Class
   4.10.5 The RecordItem Class
   4.11 The AdditionalData Class
   4.12 The History Class
   4.12.1 The HistoryItem class
   4.12.2 The DateTime Class
   4.13 The Assessment Class
   4.13.1 The Impact Class
   4.13.2 The Action Class
   4.13.3 The Confidence Class
   4.14 The Authority Class
   4.14.1 The Organization
5. **Extending the IODEF**
   5.1 Extending the Data Model
   5.2 Extending the XML DTD
6. **Special Considerations**
   6.1 XML Validity and Well-Formedness
   6.2 Unrecognized XML Tags
   6.3 Digital Signatures
7. **Examples**
8. **The IODEF Document Type Definition**
9. **References**
10. **Security Considerations**
11. **IANA Considerations**
12. **Acknowledgements**
13. **Authors' Addresses**
14. **Full Copyright Statement**

Nous ne pouvons que conseiller la lecture détaillée de ce document dont l'importance est à ne pas sous-estimer. Le modèle proposé est en effet amené à jouer un rôle notable au sein des structures d'alertes des organismes et entreprises qui, même si elles ne sont pas dotées d'un **CSIRT**, devront disposer de définitions standardisées et non ambiguës pour codifier ou remonter un incident de sécurité auprès des services ad'hoc.

ftp://ftp.nordu.net/internet-drafts/draft-ietf-inch-iodef-00.txt

ftp://ftp.nordu.net/internet-drafts/draft-meyer-inch-iodef-00.txt

http://www.terena.nl/tech/task-forces/tf-csirt/

DRAFT-IETF-INCH-IODEF-RFC3067BIS-REQUIREMENTS-00

Incident Object Description and Exchange Format Requirements

En Mars 2001, l'association **TERENA** (**T**rans-**E**uropean **R**esearch **E**ducation **N**etworking **A**ssociation) éditait le **RFC3067** sous le titre '**TERENA'S Incident Object Description and Exchange Format Requirements**' (Rapport N°32 – Mars 2001). Ce document contenait la description détaillée des termes et des contraintes applicables à la description d'un incident de sécurité, ces éléments étant décrits en accord avec les résultats des travaux du groupe **IODEF**.

Une nouvelle révision est aujourd'hui proposée à la normalisation sous un titre éliminant toute référence à l'association ayant financé les travaux. Cette nouvelle mouture de 15 pages reprend les grands principes de la version originale à quelques aménagements près dans les paragraphes 4.3, 5.1, 6.16 et 6.18.

1. Conventions used in this document
2. Introduction
   2.1 Rationale

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

2.2 Incident Description Terms
- 2.2.1 **Attack**
- 2.2.2 **Attacker**
- 2.2.3 **CSIRT**
- 2.2.4 **Damage**
- 2.2.5 **Event**
- 2.2.6 **Evidence**
- 2.2.7 **Incident**
- 2.2.8 **Impact**
- 2.2.9 **Target**
- 2.2.10 **Victim**
- 2.2.11 **Vulnerability**
- 2.2.12 Other terms

3. General Requirements

3.1 The IODEF shall reference and use previously published RFCs where possible.

4. Description Format

4.1 IODEF shall support full internationalization and localization.

4.2 The IODEF must support modularity in Incident description to allow aggregation and filtering of data.

4.3 IODEF must support the application of an access restriction policy to individual components and to individual accessing entities.

avant: *IODEF must support the application of an access restriction policy attribute to every element.*

5. Communications Mechanisms Requirements

5.1 IODEF exchange will normally be initiated by humans using standard communication protocols, for example, e-mail, HTTP, XML Web Services (based on SOAP XML Protocol).

avant: *IODEF exchange will normally be initiated by humans using standard communication protocols, for example, e-mail, WWW/HTTP, LDAP.*

6. Message Contents

6.1 The root element of the IO description should contain a unique identification number (or identifier), IO purpose and default permission level

6.2 The content of the IODEF description should contain the type of the attack if it is known.

6.3 The IODEF description must be structured such that any relevant advisories, such as those from CERT/CC, CVE, can be referenced.

6.4 IODEF may include a detailed description of the attack that caused the current Incident.

6.5 The IODEF description must include or be able to reference additional detailed data related to this specific underlying event(s)/activity, often referred as evidence.

6.6 The IODEF description MUST contain the description of the attacker and victim.

6.7 The IODEF description must support the representation of different types of device addresses, e.g., IP address (version 4 or 6) and Internet name.

6.8 IODEF must include the Identity of the creator (or current owner) of the Incident Object (CSIRT or other authority). This may be the sender in an information exchange or the team currently handling the incident.

6.9 The IODEF description must contain an indication of the possible impact of this event on the target. The value of this field should be drawn from a standardized list of values if the attack is recognized as known, or expressed in a free language by responsible CSIRT team member.

6.10. The IODEF must be able to state the degree of confidence in the report information.

6.11 The IODEF description must provide information about the actions taken in the course of this incident by previous CSIRTs.

6.12 The IODEF must support reporting of the time of all stages along Incident life-time.

6.13 Time shall be reported as the local time and time zone offset from UTC. (Note: See RFC 1902 for guidelines on reporting time.)

6.14 The format for reporting the date must be compliant with all current standards for Year 2000 rollover, and it must have sufficient capability to continue reporting date values past the year 2038.

6.15 Time granularity in IO time parameters shall not be specified by the IODEF.

6.16 The IODEF should provide the possibility to secure the confidentiality of the description content.

avant: *The IODEF should support confidentiality of the description*

6.17 The IODEF should ensure the integrity of the description content.

6.18 The IODEF should ensure the authenticity of the Incident description content.

avant: *The IODEF should ensure the authenticity and non-repudiation of the message content*

6. 19 The IODEF description must support an extension mechanism which may be used by implementers. This allows future implementation-specific or experimental data. The implementer MUST indicate how to interpret any included extensions.

6.20. The semantics of the IODEF description must be well defined.

7. IODEF extensibility

7.1. The IODEF itself MUST be extensible. It is essential that when the use of new technologies and development of automated Incident handling system demands extension of IODEF, the IODEF will be capable to include new information.

8. Security considerations

9. Acknoledgements

Nous retiendrons les définitions proposées - hélas uniquement en langue anglo-saxonne - pour les onze termes les plus couramment utilisés lors de la description d'un incident.

ftp://ftp.isi.edu/in-notes/rfc3067.txt
ftp://ftp.nordu.net/internet-drafts/draft-ietf-inch-iodef-rfc3067bis-requirements-00.txt

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ALERTES ET ATTAQUES

ALERTES

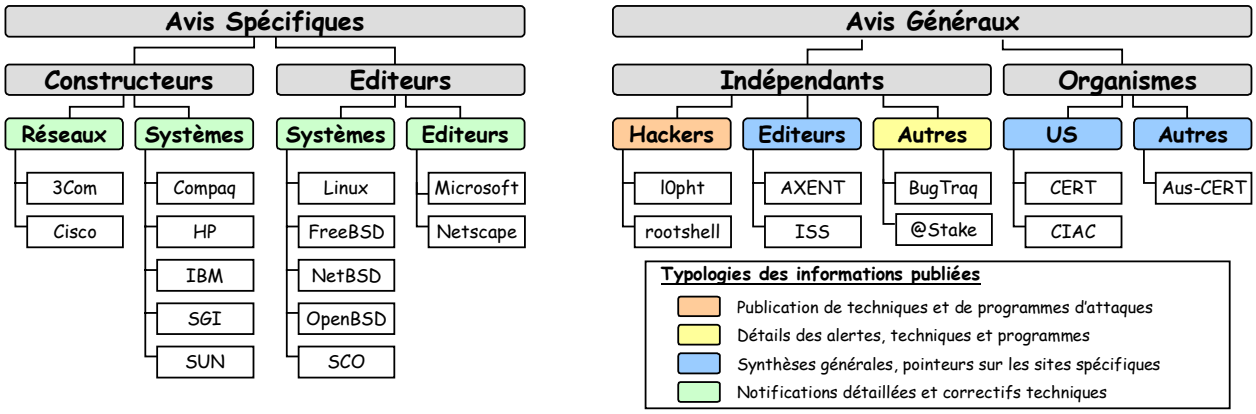
GUIDE DE LECTURE

La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

- Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,
- Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

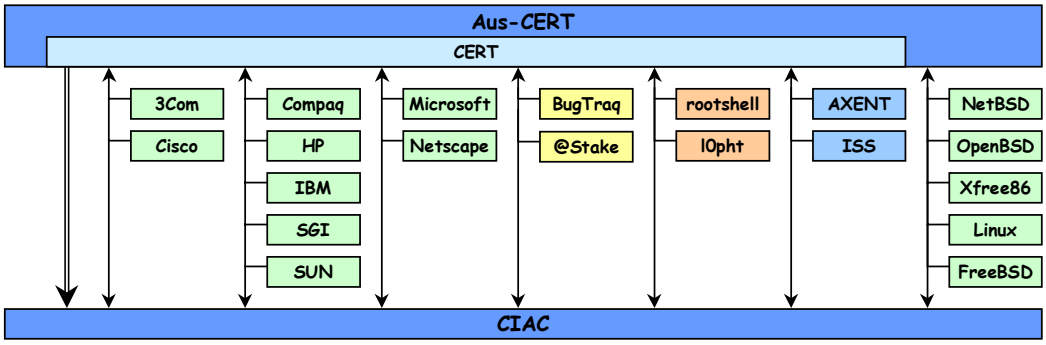
La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme d'un synoptique résumant les caractéristiques de chacune des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés.



L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

- Recherche d'informations générales et de tendances : Lecture des avis du CERT et du CIAC
- Maintenance des systèmes : Lecture des avis constructeurs associés
- Compréhension et anticipation des menaces : Lecture des avis des groupes indépendants



© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

FORMAT DE LA PRESENTATION

Les alertes et informations sont présentées classées par sources puis par niveau de gravité sous la forme de tableaux récapitulatifs constitués comme suit :

❖ Présentation des Alertes

EDITEUR

TITRE			
Description sommaire			
Gravité	Date	Informations concernant la plate-forme impactée	
Correction		Produit visé par la vulnérabilité	Description rapide de la source du problème
Référence		URL pointant sur la source la plus pertinente	

❖ Présentation des Informations

SOURCE

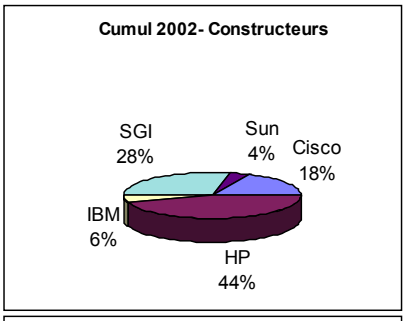
TITRE
Description sommaire
URL pointant sur la source d'information

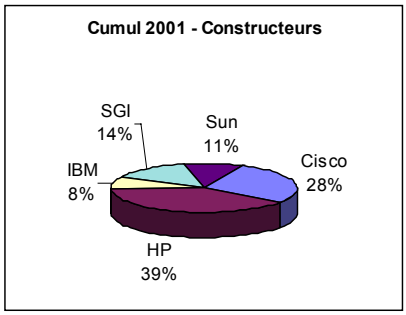
SYNTHESE MENSUELLE

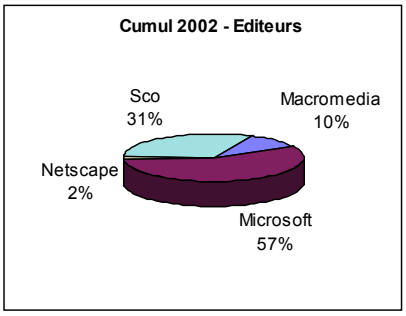
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

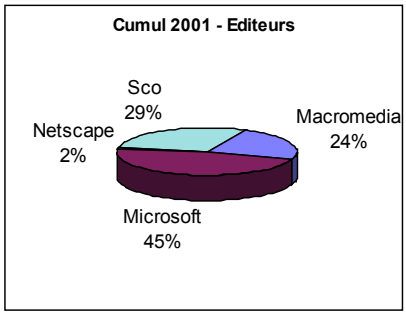
Période du **23/11/2002** au **20/12/2002**

		Cumul	
	Période	**2002**	**2001**
Organisme	**18**	**165**	**186**
CERT-CA	3	36	36
CERT-IN	2	7	15
CIAC	13	122	135
Constructeurs	**23**	**220**	**123**
Cisco	2	39	34
HP	14	99	49
IBM	1	13	10
SGI	5	61	17
Sun	1	8	13
Editeurs	**12**	**127**	**131**
Macromedia	4	13	31
Microsoft	6	72	60
Netscape	0	2	2
Sco	2	40	38
Unix libres	**32**	**349**	**340**
Linux RedHat	10	102	83
Linux Debian	13	120	94
Linux Mandr.	9	85	95
FreeBSD	0	42	68
Autres	**1**	**31**	**54**
@Stake	0	9	13
Safer	0	0	5
X-Force	1	22	36









© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ALERTES DETAILLEES

AVIS OFFICIELS

Les tables suivantes présentent une synthèse des principales alertes de sécurité émises par un organisme fiable, par l'éditeur du produit ou par le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés, s'il y en a, doivent immédiatement être appliqués.

BEA

Déni de service dans WebLogic			
La présence d'un ficher spécialement conçu sur le serveur WebLogic peut provoquer son blocage.			
Moyenne	14/12	BEA WebLogic Server et Express 6.0, 6.1, 7.0 et 7.0.0.1, BEA WebLogic Integration 2.1 et 7.0	
Correctif existant		Analyseur syntaxique 'Xerces'	Consommation excessive de mémoire
BEA02-23.01		http://dev2dev.bea.com/resourcelibrary/advisoriesdetail.jsp	

CISCO

Déni de service contre les cartes optiques			
Il est possible de provoquer le blocage d'un port optique.			
Faible	11/12	Module OSM sur un Catalyst utilisant une version 12.(8)E à 12.1(13.4)E de l'IOS.	
Correctif existant		Module optique	Traitement des trames invalides
CSCdy29717		http://www.cisco.com/warp/public/707/osm-lc-ios-pkt-vuln-pub.shtml	

Vulnérabilité dans l'implémentation SSH des IOS			
L'implémentation SSH des routeurs et commutateurs utilisant l'IOS est vulnérable à un déni de service			
Forte	19/12	Routeurs et commutateurs utilisant un IOS 12.0S, 12.0ST,12.1T, 12.1E, 12.2, 12.2T ou 12.2S	
Correctif existant		Serveur SSH embarqué	Non disponible
CSCdz60229		http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml	

HP

Débordement dans le serveur de polices de caractères			
Le serveur de polices de caractères fourni avec HP-UX contient un débordement de buffer.			
Critique	04/12	HP-UX 10.10 à 11.22	
Correctif existant		Programme 'fs.auto'	Débordement de buffer
HPSBUX0212-228		http://europe-support.external.hp.com/	

Débordement de buffer dans CIFS			
Le serveur CIFS est un portage de Samba sur HP 9000 et est sujet au même débordement de buffer que celui-ci.			
Forte	10/12	HP 9000 utilisant l'une des versions suivantes de CIFS 2.2:A.01.08, A.01.08.01 ou A.01.09	
Correctif existant		Vérification du mot de passe	Mauvaise vérification de la longueur du mot de passe
HPSBUX0212-230		http://europe-support2.external.hp.com/	

Vulnérabilité dans 'ied'			
Une vulnérabilité dans 'ied' permet d'accéder à des données protégées.			
Moyenne	03/12	HP-UX 10.10, 10.20 et 11.00	
Correctif existant		Programme 'ied'	Non disponible
HPSBUX0212-227		http://www.itrc.hp.com/	

Droits incorrects sur certains fichiers			
Certains répertoires de 'Visualize Conference' possèdent des droits trop laxistes.			
Moyenne	10/12	HP-UX 10.00 et 11.11 avec HP-UX Visualize ConferenceB.11.00.11	
Correctif existant		Installation du logiciel	Droits laxistes
HPSBUX0212-231		http://europe-support2.external.hp.com/	

Instabilité du service 'xntpd'			
Le service 'xntpd' sur HP-UX peut provoquer un ralentissement, voire le blocage du système.			
Moyenne	10/12	HP-UX 10.20, 10.24, 11.00, 11.04 et 11.11	
Correctif existant		Service 'xntpd'	Non disponible
HPSBUX0212-232		http://europe-support2.external.hp.com/	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

HP/COMPAQ

Vulnérabilité dans Tru64

Il est possible à un utilisateur de compromettre le système de fichiers de Tru64.

Forte	25/11	HP/Compaq Tru64 4.0f, 4.0g, 5.0a, 5.1 et 5.1a	
Correctif existant		uudecode	Non disponible
SSRT2301		http://wwss1pro.compaq.com/.../viewdocument.asp?prodid=811&source=SRB0031W.xml&docid=13225	

Vulnérabilités dans OSIS

Une vulnérabilité a été découverte dans OSIS pour Tru64

Faible	13/11	HP/Compaq OSIS 5.4 sur Tru64 4.0f et 4.0g	
Correctif existant		Module d'authentification LDAP	Non disponible
SSRT2385		http://wwss1pro.compaq.com/.../viewdocument.asp?prodid=117&source=SRB0061W.xmldocid=13014	

IBM

Débordement de buffer dans CDE

Un débordement de buffer a été découvert dans CDE sur AIX.

Forte	02/12	IBM AIX 4.3.3 et 5.1.0	
Correctif existant		Bibliothèque 'dtsvc'	Débordement de buffer
IY24596,IY25504		http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2002.1060.1	

LINUX CALDERA

Débordement de buffer dans 'nss_ldap'

Le paquetage 'nss_ldap' contient un débordement de buffer dans le traitement des requêtes DNS.

Critique	10/12	Caldera OpenLinux 3.1 et 3.1.1 avec un paquetage 'nss_ldap' de version inférieure à la 172.5	
Correctif existant		Paquetage 'nss_ldap'	Débordement de buffer
CSSA-2002-058.0		ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2002-058.0.txt	

LINUX DEBIAN

Vulnérabilité dans 'smb2www'

Une vulnérabilité existe dans 'smb2www', utilisé pour parcourir un réseau SMB depuis un navigateur web.

Forte	04/12	smb2www versions précédentes à 980804-16.1, 980804-8.1 et 980804-17	
Correctif existant		smb2www	Non disponible
DSA-203-1		http://www.debian.org/security/2002/dsa-203	

Vulnérabilité dans 'im'

Les programmes du paquetage 'im', qui fournit des outils pour gérer les e-mail et les forums de discussion, créent des fichiers de façon non sécurisée.

Moyenne	03/12	IM versions inférieures à 133-2.2, 141-18.1 et 141-20	
Correctif existant		'impwagent' et 'immknmz'	Création de fichiers et de répertoires temporaires de manière non sécurisée
DSA-202-1		http://www.debian.org/security/2002/dsa-202	

Débordement de buffer dans 'libpng'

Un débordement de buffer a été découvert dans la bibliothèque 'libpng'.

Forte	19/12	Versions de libpng inférieures à la 1.0.12-3.woody.3,1.2.1-1.1.woody.3 ou 1.0.5-1.1	
Correctif existant		Bibliothèque 'libpng'	Débordement de buffer
DSA-213-1		http://www.debian.org/security/2002/dsa-213	

LINUX REDHAT

Déni de service dans le noyau

Red Hat a publié un nouveau noyau 2.2, qui résout des problèmes de déni de service.

Moyenne	25/11	Red Hat 6.2 et 7.0 sur architecture Intel 32 bits	
Correctif existant		Noyau	Non disponible
RHSA-02:264-05		http://rhn.redhat.com/errata/RHSA-2002-262.html	

Déni de service contre l'agent SNMP

Un déni de service contre l'agent SNMP fourni avec Red Hat a été découvert.

Faible	17/12	Net-SNMP 5.0.1 à 5.0.4, fourni avec Red Hat 8.0	
Correctif existant		Agent SNMP	Non disponible
RHSA-02:228-11		http://rhn.redhat.com/errata/RHSA-2002-228.html	

LINUX SUSE

Vulnérabilité dans OpenLDAP

Il existe une vulnérabilité dans la version d'OpenLDAP fournie avec SuSE.

Forte	06/12	SuSE 7.1, 7.2, 7.3 et 8.0 utilisant OpenLDAP	
Correctif existant		OpenLDAP	Débordements de buffer
SuSE-SA:02:047		http://www.suse.de/de/security/2002_047_openldap2.html	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

MACROMEDIA

Débordement de buffer dans 'Flash player'

Un nouveau débordement de buffer a été découvert dans 'Flash player'.

Forte	16/12	Macromedia Flash Player versions inférieures à 6.0.65.0	
Correctif existant		Décodage des fichiers 'SWF'	Débordement de buffer
AD20021216		http://www.eeye.com/html/Research/Advisories/AD20021216.html	
MPSB02-15		http://www.macromedia.com/v1/handlers/index.cfm?ID=23569	

MICROSOFT

Vulnérabilités dans la machine virtuelle java

Plusieurs vulnérabilités ont été découvertes dans la machine virtuelle java de Microsoft.

Critique	11/12	Microsoft Windows utilisant une version de JVM inférieure à la 3809	
Correctif existant		Machine virtuelle java	Multiples vulnérabilités
MS02-069		http://www.microsoft.com/technet/security/bulletin/MS02-069.asp	

Faille dans l'implémentation SMB

Une faille dans l'implémentation de SMB permet de supprimer la signature des paquets SMB.

Forte	11/12	Microsoft Windows 2000 et XP	
Correctif existant		Protocole SMB	Erreur d'implémentation
MS02-070		http://www.microsoft.com/technet/security/bulletin/MS02-070.asp	

Vulnérabilité dans les signaux 'WM_TIMER'

Il est possible d'utiliser les signaux 'WM_TIMER' pour provoquer l'exécution de code par des applications tierces.

Forte	11/12	Microsoft Windows NT 4.0, 2000 et XP	
Correctif existant		Communication inter-processus	Envoi de messages à des applications tierces
MS02-071		http://www.microsoft.com/technet/security/bulletin/MS02-071.asp	

Vulnérabilité dans Windows XP

Un débordement de buffer existe dans l'interface de Windows XP.

Forte	18/12	Microsoft Windows XP	
Correctif existant		Interface utilisateur	Débordement de buffer
MS02-072		http://www.microsoft.com/technet/security/bulletin/MS02-072.asp	
CA-2002-37		http://www.cert.org/advisories/CA-2002-37.html	
N-072		http://www.ciac.org/ciac/bulletins/n-029.shtml	

Vulnérabilité dans Internet Explorer

Il est possible de contourner le mécanisme de cloisonnement des domaines d'Internet Explorer.

Moyenne	04/12	Microsoft Internet Explorer 5.5 et 6.0	
Correctif existant		Internet Explorer	Erreur d'implémentation
MS02-068		http://www.microsoft.com/technet/security/bulletin/MS02-068.asp	

Déni de service contre Outlook

Il est possible de provoquer le blocage d'Outlook avec certains messages.

Faible	04/12	Microsoft Outlook 2002	
Correctif existant		Outlook	Mauvais traitement des en-têtes
MS02-067		http://www.microsoft.com/technet/security/bulletin/MS02-067.asp	

NETSCREEN

Contournement du filtrage d'URL

Il est possible de contourner la fonctionnalité de filtrage d'URL de Netscreen.

Forte	25/11	NetScreen utilisant une version de ScreenOS inférieure ou égale à la 4.0	
Correctif existant		Analyseur d'URL	Insuffisance de la fonction de ré-assemblage de paquets
Netscreen		http://online.securityfocus.com/archive/1/301029	

Prédictibilité des numéros de séquence TCP

Le pare-feu Netscreen génère des numéros de séquences prédictibles.

Forte	25/11	Netscreen utilisant une version de ScreenOS inférieure ou égale à la 4.0	
Correctif existant		Numéros de séquence	Prédictibilité des numéros de séquences TCP
Netscreen		http://www.netscreen.com/support/alerts/Predictable_TCP_Initial_Sequence_Numbers.html	

Déni de service par H.323

Il est possible de provoquer la saturation de la table d'état d'un pare-feu Netscreen autorisant le protocole H.323.

Forte	25/11	Netscreen utilisant ScreenOS 2.8, 3.0, 3.1 et 4.0	
Correctif existant		Table de sessions	Maintien de sessions plus longtemps que nécessaire
Netscreen		http://www.netscreen.com/support/alerts/Potential_H_323_Denial_of_Service.html	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

SCO

Vulnérabilité dans UnixWare et OpenUNIX

Il est possible d'accéder aux fichiers protégés du système.

Forte	09/12	SCO UnixWare 7.1.1 et OpenUNIX 8.0.0	
Correctif existant		Noyau	Mauvaise gestion des descripteurs de fichiers
CSSA-02-SCO.43		ftp://ftp.sco.com/pub/updates/OpenUNIX/CSSA-2002-SCO.43/CSSA-2002-SCO.43.txt	

Vulnérabilité de 'uudecode'

Une vulnérabilité de l'utilitaire 'uudecode' permet d'obtenir des privilèges élevés ou d'écraser certains fichiers sensibles.

Forte	11/12	SCO UnixWare 7.1.1 et Open UNIX 8.0.0	
Correctif existant		Utilitaire 'uudecode'	Suivi de lien symbolique
CSSA-02-SCO.44		ftp://ftp.sco.com/pub/updates/OpenUNIX/CSSA-2002-SCO.44/CSSA-2002-SCO.44.txt	

SGI

Débordement dans le serveur de polices de caractères

Le serveur de polices de caractères fourni avec IRIX contient un débordement de buffer.

Critique	04/12	SGI IRIX 6.5.13 et précédents	
Correctif existant		Programme 'fs.auto'	Débordement de buffer
20021202-01-I		ftp://patches.sgi.com/support/free/security/advisories/20021202-01-I	

SSH

Vulnérabilités dans plusieurs implémentations

Plusieurs implémentations de SSH contiennent des vulnérabilités dans le client et le serveur.

Critique	16/12	F-Secure SSH 3.1.0 build 11 pour Unix et 5.2 pour Windows InterSoft Secure NetTerm client 5.4.1 NetComposite ShellGuard SSH client 3.4.6 PuTTY 0.53WinSCP SCP 2.0.0	SSH Communications SSH 3.2.2 FiSSH SSH client 1.0A Pragma SSH server 2 WinSCP SCP V2.0 pour Windows
Correctif existant		Clients et serveurs SSH	Divers
Rapid 7		http://www.rapid7.com/advisories/R7-0009.txt	
CA-2002-36		http://www.cert.org/advisories/CA-2002-36.html	

Vulnérabilité dans le serveur de SSH Communications

Le serveur SSH de SSH Communications indique root comme nom de login des utilisateurs.

Forte	25/11	SSH Communications SSH 2.0.13 à 3.1.4, 3.2 et 3.2.1	
Correctif existant		Serveur SSH	Mauvais détachement du processus
VU#740619		http://www.kb.cert.org/vuls/id/740619	
SSH Comm.		http://www.ssh.com/company/newsroom/article/286/	

SUN

Débordement dans le serveur de polices de caractères

Le serveurs de polices de caractères fourni avec Solaris contient un débordement de buffer.

Critique	25/11	Sun Solaris 2.5.1 à 9	
Correctif existant		'/usr/openwin/lib/fs.auto'	Débordement de buffer
CA-2002-34		http://www.cert.org/advisories/CA-2002-34.html	
ISS		http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21541	

Vulnérabilité dans Cobalt RaQ 4

Il existe une vulnérabilité dans l'interface d'administration web des serveurs RaQ.

Forte	05/12	Sun Cobalt RaQ 4 avec le paquetage de sécurisation	
Correctif existant		Serveur web d'administration	Mauvais filtrage des paramètres
BID 6326		http://online.securityfocus.com/bid/6326	
CERT		http://www.cert.org/advisories/CA-2002-35.html	

Vulnérabilité dans 'priocntl'

Une vulnérabilité dans l'appel système 'priocntl' permet à un utilisateur local d'acquérir les privilèges root.

Forte	28/11	Sun Solaris 2.5.1 à 9	
Aucun correctif		Appel système 'priocntl'	Non vérification d'argument
Alert ID 49131		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/49131	

Déni de service local

Il est possible à un utilisateur local de rendre le système inutilisable.

Faible	02/12	Sun Solaris 2.5.1 à 9	
Correctif existant		Noyau	Mauvaise gestion des exceptions
Alert ID 48267		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/48267	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Défaut d'initialisation dans la machine virtuelle Java			
Un problème dans la machine virtuelle peut conduire à l'instanciation d'objets imparfaitement initialisés.			
Faible	09/12	SDK et JRE 1.4.1 SDK et JRE 1.3.1_05 ou plus ancien SDK et JRE 1.2.2_013 ou plus ancien	SDK et JRE 1.4.0_02 ou plus ancien SDK et JRE 1.3.0_05 ou plus ancien JDK et JRE 1.1.xsur plates-formes Windows et Unix
Correctif existant		Vérificateur de code java	Mauvaise initialisation des instances
Alert ID 49304		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/49304	

Déni de service contre 'mailtool'			
Il est possible de provoquer un déni de service contre les utilisateurs de 'mailtool'.			
Faible	16/12	Sun Solaris 2.5.1, 2.6, 7 et 8	
Correctif existant		Utilitaire 'mailtool'	Débordement de buffer
Alert ID 48216		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/48216	

TREND MICRO

Vulnérabilité dans PC-Cillin			
PC-Cillin contient une vulnérabilité dans son proxy POP3.			
Forte	10/12	PC-cillin 2000, 2002 et 2003, OfficeScan Corporate Edition	
Correctif existant		Proxy POP3	Débordement de buffer
Trend Micro		http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionId=12982	
Bugtraq		http://online.securityfocus.com/archive/1/302753	

WGet

Vulnérabilité dans plusieurs clients FTP			
Plusieurs clients FTP sont vulnérables à un déréférencement de répertoire.			
Faible	11/12	wget versions 1.7.1 et 1.8.1Clients fournis avec OpenBSD 3.0 et Solaris 2.6 et 7	
Correctif existant		Clients FTP	Déréférencement de répertoire
RHSA-2002-229		http://www.redhat.com/support/errata/RHSA-2002-229.html	
Securiteam		http://www.securiteam.com/securitynews/6G00B0A6AC.html	

ALERTES NON CONFIRMEES

Les alertes présentées dans les tables de synthèse suivantes ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une annonce ou d'un correctif de la part de l'éditeur. Ces alertes nécessitent la mise en place d'un processus de suivi et d'observation.

APACHE

Vulnérabilité dans le serveur Tomcat			
Le serveur Tomcat contient une vulnérabilité pouvant conduire à la divulgation d'informations privées.			
Forte	05/12	Tomcat 4.x utilisant Apache 1.3.x, 'mod_jk' 1.2 et AJP 1.3	
Correctif existant		Module 'mod_jk'	Désynchronisation des composants du serveur
Bugtraq		http://online.securityfocus.com/archive/1/302169	

FETCHMAIL

Vulnérabilité dans Fetchmail			
Il est possible de provoquer l'exécution de code par 'Fetchmail'.			
Critique	13/12	Fetchmail 6.1.3 et précédents	
Correctif existant		Adresses destination	Débordement de buffer
Bugtraq		http://online.securityfocus.com/archive/1/303282	

LINKSYS

Déni de service contre des routeurs Linksys			
Il est possible de provoquer un déni de service contre certains routeurs Linksys en utilisant l'interface web.			
Moyenne	19/11	Linksys BEFW11S4, BEFSR11, BEFSR41 et BEFSRU31 avec une version de firmware inférieure à la 1.43.3	
Correctif existant		Serveur HTTP embarqué	Débordement de buffer
iDEFENSE		http://www.idefense.com/advisory/11.19.02a.txt	

MACROMEDIA

Attaque de type 'cross-site scripting' dans ColdFusion			
Une vulnérabilité de type 'cross-site scripting' a été découverte dans ColdFusion.			
Forte	16/12	Macromedia ColdFusion 5.0	
Aucun correctif		Visualisation des journaux	Non échappement des données
Bugtraq		http://online.securityfocus.com/archive/1/303545	

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

MYPHPLINKS

Contournement de l'authentification			
Il est possible de contourner l'authentification de MyPHPLinks par une technique d'injection de code SQL.			
Forte	14/12	MyPHP Links 2.1.9 et 2.2.0 et probablement des versions inférieures	
Correctif existant		Fichier 'auth/checksession.php'	Injection de code SQL
Bugtraq		http://online.securityfocus.com/archive/1/303379	

MYSQL

Multiples vulnérabilités dans MySQL			
Plusieurs vulnérabilités ont été découvertes, à la fois dans le serveur et le client de MySQL.			
Critique	12/12	MySQL, serveur et client, jusqu'à la version 3.23.53a, ou la version 4.0.5a	
Correctif existant		MySQL	Débordement de buffer
E-Matters		http://security.e-matters.de/advisories/042002.html	

SYBASE

Multiples vulnérabilités dans Sybase			
Plusieurs vulnérabilités concernant Sybase ont été publiées.			
Forte	26/11	Sybase Adaptive server 12.0 et 12.5	
Correctif existant		'DBCC CHECKVERIFY', 'DROP DATABASE' et 'xp_freedll'	Débordements de buffer
Application Sec.		http://www.appsecinc.com/resources/alerts/sybase/02-0001.html	

SYMANTEC

Vulnérabilité dans Entreprise Firewall			
Une vulnérabilité a été découverte dans le proxy Real Audio			
Critique	13/12	Symantec Raptor 6.5 et 6.5.3, Entreprise Firewall 6.5.2 et 7.0, Gateway Security 5110, 2500 et 5300, VelociRaptor 500, 700, 1000, 1100, 1200 et 1300	
Correctif existant		Proxy Real Audio	Débordement de buffer
BID 6389		http://online.securityfocus.com/bid/6389	

TRACEROUTE NG

Débordements de buffer dans 'traceroute-ng'			
Il existe plusieurs débordements de buffer dans le logiciel 'traceroute-ng'.			
Moyenne	01/12	Traceroute NG	
Aucun correctif		Traceroute NG	Débordements de buffer
Securiteam		http://www.securiteam.com/unixfocus/6W0080A6AC.html	

TRENDMICRO

Rebond par InterScan VirusWall			
Il est possible d'utiliser le proxy HTTP inclus dans InterScan VirusWall pour rebondir vers d'autres adresses et ports.			
Forte	05/12	TrendMicro InterScan VirusWall V3.6	
Correctif existant		Proxy HTTP	Les requêtes 'CONNECT' ne sont pas filtrées.
Bugtraq		http://online.securityfocus.com/archive/1/302200	

WINAMP

Débordement de buffer dans la lecture des fichiers			
Winamp est sujet à un débordement de buffer lors de l'analyse des fichiers '.mp3'			
Moyenne	18/12	Winamp 2.81 et 3.0	
Correctif existant		Informations du fichier	Débordement de buffer
FS2002-10		http://www.foundstone.com/knowledge/randd-advisories-display.html?id=338	

AUTRES INFORMATIONS

REPRISES D'AVIS ET CORRECTIFS

Les vulnérabilités suivantes, déjà publiées, ont été mises à jour, reprises par un autre organisme, ou ont donné lieu à la fourniture d'un correctif :

CIAC

Reprise de l'avis Red Hat sur Samba
Le CIAC a repris, sous la référence [N-019], l'avis de Red Hat sur un débordement de buffer dans Samba.
http://www.ciac.org/ciac/bulletins/n-019.shtml

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Reprise de l'avis Microsoft MS02-068

Le CIAC a repris, sous la référence N-021, l'avis Microsoft concernant une vulnérabilité dans Internet Explorer.

http://www.ciac.org/ciac/bulletins/n-021.shtml

Reprise de l'avis Red Hat RHSA-2002:229-10

Le CIAC a repris, sous la référence [N-022], l'avis de Red Hat concernant 'wget'.

http://www.ciac.org/ciac/bulletins/n-022.shtml

Reprise de l'avis HP HPSBUX0212-230

Le CIAC a repris, sous la référence [N-023], l'avis de HP a propos du serveur CIFS. HP [HPSBUX0212-230]

http://www.ciac.org/ciac/bulletins/n-023.shtml

Reprise de l'avis CERT CA-2002-34

Le CIAC a repris, sous la référence [N-024], l'avis du CERT concernant une vulnérabilité dans le serveur de polices de caractères de Solaris.

http://www.ciac.org/ciac/bulletins/n-024.shtml

Reprise de l'avis CERT CA-2002-35

Le CIAC a repris, sous la référence [N-025], l'avis du CERT concernant les serveur RaQ 4 de Sun/Cobalt.

http://www.ciac.org/ciac/bulletins/n-025.shtml

Reprise de l'avis Microsoft MS02-069

Le CIAC a repris sous la référence [N-026] l'avis de Microsoft concernant plusieurs failles dans sa machine virtuelle java.

http://www.ciac.org/ciac/bulletins/n-026.shtml

Reprise de l'avis Microsoft MS02-071

Le CIAC a repris, sous la référence [N-027], l'avis Microsoft concernant les signaux 'WM_TIMER'.

http://www.ciac.org/ciac/bulletins/n-027.shtml

Reprise de l'avis de Rapid 7 sur SSH

Le CIAC a repris sous la référence [N-028] l'avis de Rapid 7 concernant des vulnérabilités dans plusieurs implémentations de SSH.

http://www.ciac.org/ciac/bulletins/n-028.shtml

Reprise de l'avis Microsoft MS02-072

Le CIAC a repris, sous la référence [N-029], l'avis de Microsoft concernant un débordement de buffer dans l'interface utilisateur de Windows XP.

http://www.ciac.org/ciac/bulletins/n-029.shtml

Reprise de l'avis HP HPSBUX0212-234

Le CIAC a repris, sous la référence [N-030], l'avis de HP concernant l'interpréteur de commande restreint de Sendmail.

http://www.ciac.org/ciac/bulletins/n-030.shtml

FREEBSD

Disponibilité de plusieurs correctifs

FreeBSD annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

bind FreeBSD-SA-02:43

http://www.linuxsecurity.com/advisories/freebsd.html

HP

Disponibilité de correctifs pour la bibliothèque XDR

HP a publié des correctifs pour la bibliothèque XDR de ses systèmes HP-UX. Depuis la précédente alerte, la liste des versions vulnérables a été étendue. La dernière liste de versions vulnérables comprend HP-UX 10.20, 10.24, 11.00, 11.04, 11.11, et 11.22.

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0209-215

Nouveaux correctifs pour 'XFS'

HP a révisé son bulletin HPSBUX0212-228 pour prévenir ses utilisateurs que les correctifs précédents contenaient une erreur. De nouveaux correctifs sont disponibles.

http://europe-support.external.hp.com/

Publication d'un avis concernant Tomcat

HP a publié un avis pour avertir ses utilisateurs d'une faille dans la configuration par défaut du serveur Tomcat, inclus dans HP-UX 11.04 avec VirtualVault A.04.60. La solution consiste à modifier la configuration comme proposé, ou de télécharger une version récente (4.0.6 ou supérieur) de Tomcat.

http://europe-support.external.hp.com/

Correctifs pour le résolveur DNS

HP a publié des correctifs pour les bibliothèques fournies avec Bind 4.9.7 et 8.1.2.

http://europe-support2.external.hp.com/

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Correctif pour 'smrsh'

HP a publié un correctif pour l'interpréteur de commande de Sendmail dont les protections pouvaient être contournées.

http://europe-support2.external.hp.com/

Correctifs pour la machine virtuelle java

HP a publié des correctifs pour les versions 1.2, 1.3 et 1.4 de la machine virtuelle java. Les versions immunes sont 1.2.2.14, 1.3.1.08 et 1.4.0.03 et sont téléchargeables via : http://www.hp.com/go/java

http://europe-support.external.hp.com/

IBM

Correctif pour le résolveur DNS

IBM a publié un correctif pour le résolveur DNS de son système AIX 4.3.3.

http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2002.1062.1

LINUX CALDERA

Disponibilité de nombreux correctifs

Caldera annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

lynx	*CSSA-2002-049.0*
fetchmail	*CSSA-2002-051.0*
smrsh	*CSSA-2002-052.0*
ypserv	*CSSA-2002-054.0*
rpc xdr	*CSSA-2002-055.0*
apache	*CSSA-2002-056.0*
groff	*CSSA-2002-057.0*
nss ldap	*CSSA-2002-058.0*

http://www.linuxsecurity.com/advisories/caldera.html

LINUX DEBIAN

Disponibilité de nombreux correctifs

Debian annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

samba	*DSA-200-1*
freeswan	*DSA-201-1*
im	*DSA-202-1*
smb2www	*DSA-203-1*
kdelibs	*DSA-204-1*
gtetrinet	*DSA-205-1*
tcpdump	*DSA-206-1*
tetex-bin	*DSA-207-1*
perl	*DSA-208-1*
wget	*DSA-209-1*
lynx	*DSA-210-1*
micq	*DSA-211-1*
mysql	*DSA-212-1*

http://www.debian.org/security/2002/

LINUX MANDRAKE

Disponibilité de nombreux correctifs

Mandrake annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

kde	*MDKSA-2002:079*	*9.0*
kdenetwork	*MDKSA-2002:080*	*9.0*
samba	*MDKSA-2002:081*	*8.1 / 8. 2 / 9.0*
python	*MDKSA-2002:082*	*7.2 / 8.0 / 8.1 / 8. 2 / 9.0 / FW 7.2*
sendmail	*MDKSA-2002:083*	*7.2 / 8.0 / 8.1 / 8. 2 / 9.0*
pine	*MDKSA-2002:084*	*7.2 / 8.0 / 8.1 / 8. 2 / 9.0*
WindowsMaker	*MDKSA-2002:085*	*7.2 / 8.0 / 8.1 / 8. 2 / 9.0*
wget	*MDKSA-2002:086*	*7.2 / 8.0 / 8.1 / 8. 2 / 9.0 / FW 7.2*
mysql	*MDKSA-2002:087*	*7.2 / 8.0 / 8.1 / 8. 2 / 9.0 / FW 7.2*

http://www.linux-mandrake.com/en/security/

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

LINUX REDHAT

Disponibilité de nombreux correctifs

RedHat annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

KDE	RHSA-2002:220-40	7.2 / 7.3 / 8.0
apache	RHSA-2002:222-21	6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0
net-snmp	RHSA-2002:228-11	8.0
wget	RHSA-2002:229-10	6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0
canna	RHSA-2002:246-18	7.1 / 7.2 / 7.3 / 8.0
webaliser	RHSA-2002:254-05	7.2
xinetd	RHSA-2002:262-07	7.0 / 7.1 / 7.2 / 7.3 / 8.0
kernel2.2	RHSA-2002:264-05	6.2 / 7.0
samba	RHSA-2002:266-05	6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0
fetchmail	RHSA-2002:293-09	6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0

http://www.linuxsecurity.com/advisories/redhat.html

SGI

Correctif pour BIND

SGI a annoncé la disponibilité d'un correctif pour le serveur DNS BIND, sujet à plusieurs vulnérabilités.

ftp://patches.sgi.com/support/free/security/advisories/20021201-01-P

Informations sur Samba

SGI a publié un avis avertissant ses utilisateurs de l'existence d'une faille de sécurité dans Samba. Les versions d'IRIX jusqu'à la 6.5.18 sont concernées. SGI ne fournit pas de correctif mais recommande l'installation de la version 2.2.7 de Samba.

http://online.securityfocus.com/archive/1/302235

SUN

Correctifs pour NIS

SUN a publié des correctifs pour NIS, dont le programme 'ypxfrd' permettait d'accéder aux fichiers systèmes. Les correctifs sont actuellement disponibles pour Solaris 2.5.1, 2.6, 8 et 9.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/47903

Solution temporaire pour iPlanet

SUN a publié une notification d'alerte concernant iPlanet 4.1. Celle-ci confirme la présence d'une vulnérabilité à la lecture des fichiers de journalisation et propose une solution temporaire consistant à interdire l'utilisation du serveur d'administration pour la visualisation de ces journaux.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/49475

CODES D'EXPLOITATION

Les codes d'exploitation des vulnérabilités suivantes ont fait l'objet d'une large diffusion :

ORACLE

Disponibilité d'un code d'exploitation

Un code d'exploitation pour une vulnérabilité touchant Oracle Listener a été publié sur Securiteam. Ce code ouvre un interpréteur de commande en écoute sur le port 8080 et est annoncé efficace contre la version 8.1.7 d'Oracle. La vulnérabilité exploitée semble être celle publiée en juin 2001.

http://www.securiteam.com/exploits/6Q00R2060S.html

BULLETINS ET NOTES

Les bulletins d'information suivants ont été publiés par les organismes officiels de surveillance et les éditeurs :

CERT

Publication de la synthèse trimestrielle [CS-2002-04]

Le CERT publie, sous la référence CS-2002-04, la synthèse des mois de septembre, octobre et novembre 2002. Cette synthèse traite des vulnérabilités, exploitations ou attaques dont il a été question ces trois derniers mois :

1. *Multiples vulnérabilités dans OpenSSL, et le ver Slapper [CA-2002-23] [CA-2002-27]*
2. *Cheval de Troie dans la distribution Sendmail [CA-2002-28]*
3. *Cheval de Troie dans Tcpdump et Libpcap [CA-2002-30]*
4. *Multiples vulnérabilités dans BIND [CA-2002-31]*
5. *Débordement de buffer dans Microsoft MDAC [CA-2002-33]*

Notons que ne sont pas évoqués les avis [CA-2002-29], [CA-2002-32] et [CA-2002-34] portant respectivement sur Kerberos, Alcatel OmniSwitch et Solaris XFS.

http://www.cert.org/summaries/CS-2002-04.html

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

VIRUS

Propagation du ver 'W32/Lioten'

Le CERT a publié une note indiquant un grand nombre de compromissions de systèmes Windows 2000 et XP par un ver nommé 'W32/Lioten'. Celui-ci se propage grâce aux partages de fichiers de Windows 2000 et s'installe dans le répertoire 'C:' sous le nom 'iraq_oil.exe'. Il semble cependant qu'il puisse s'installer sous un autre nom ou dans un autre répertoire. Une forte activité sur le port 445/tcp peut être le signe d'une machine compromise qui tente de propager ce ver.

http://www.cert.org/incident_notes/IN-2002-06.html

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

ATTAQUES

OUTILS

PAKETTO KEIRETSU

▪ **Description**

Dénommé '**Paketto Keiretsu**', ce paquetage contient 5 outils d'analyse fonctionnant en environnement UNIX et utilisant des techniques pour le moins inhabituelles. Ces techniques ont été décrites à l'occasion de la présentation '**BLACK OPS OF TCP/IP**' lors de la conférence '**HiverCON 2002**' qui s'est tenu à **DUBLIN** fin Novembre. La lecture de cette présentation de 81 pages au format 'Power Point' est à notre point de vue absolument indispensable. Les techniques révélées sont en effet susceptibles de remettre en cause bon nombre d'idées reçues et par conséquence, de fragiliser certains mécanismes de sécurité mis en œuvre dans les dispositifs de filtrages.

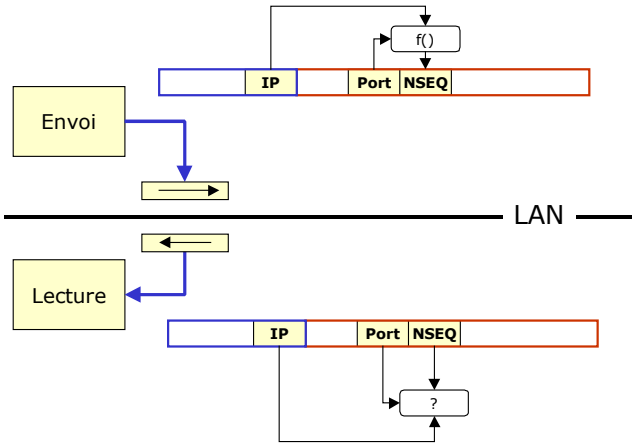
▪ **scanrand**

Si la fonction de sondage des services actifs sur **TCP** proposée par cet utilitaire est somme toute banale, la technique employée l'est moins, les performances étant, elles, extraordinaires. En effet, la fonction d'émission d'un paquet **TCP** d'ouverture de connexion dit '**TCP SYN**' est complètement dissociée de celle chargée de recevoir l'éventuelle réponse, à savoir un paquet **TCP** dit '**SYN/ACK**'.

Cette technique permet d'atteindre d'excellentes performances en terme de vitesse de sondage, le programme n'étant nullement tenu d'attendre soit l'éventuelle réponse, soit l'échéance d'un temps de garde, avant d'engager le prochain sondage. Jusqu'alors, les programmes implémentant une telle technique utilisaient les paramètres contextuels présents dans le paquet réponse dont l'adresse IP et le port destination de la cible comme clef de référence.

Dans le cas de '**scanrand**', l'auteur a décidé d'implémenter une vérification complémentaire en transmettant une somme cryptographique élaborée à partir de l'adresse IP et du port destination dans le champ contenant le numéro de séquence TCP.

Ce procédé respecte parfaitement les spécifications du protocole TCP, lesquelles laissent le choix du numéro de séquence à l'initiateur de la session.



Lors de la réception du paquet d'acquittement '**SYN/ACK**', la fonction de traitement effectue la même opération à partir de l'adresse IP et du numéro de port contenu dans le paquet reçu et contrôle la validité du numéro de séquence préalablement décrémenté.

```
# ./scanrand -b10M 10.A.B.1-253:80,20-22,1433
  UP:       10.A.B.14:80     [01]    0.259s
  UP:       10.A.B.43:80     [01]    0.839s
  UP:       10.A.B.50:80     [01]    0.979s
  UP:       10.A.B.54:80     [01]    1.059s
  UP:       10.A.B.14:1433   [01]    5.319s
  UP:       10.A.B.18:1433   [01]    5.399s
  UP:       10.A.B.56:1433   [01]    6.160s
  UP:       10.A.B.77:1433   [01]    6.580s
```

Cet exemple montre la mise en œuvre de '**scanrand**' pour rechercher les postes sur lesquels les services WEB (port 80) ou SQL-Server (1433) sont actifs.

La dernière colonne contient une estimation du temps écoulé entre l'envoi du paquet initial et la réception de la réponse.

Les adresses originales ont bien entendu été masquées …

On notera que le procédé employé ne conservant aucun état intermédiaire permettant d'associer le paquet émis et la réponse reçue (mécanisme dit 'asynchronous stateless'), les résultats apparaissent dans l'ordre de la réception d'une réponse en provenance de chaque service testé. L'utilisateur devra réordonnancer ces résultats pour obtenir la liste des différents services actifs sur une même adresse IP (un simple tri par le biais de la commande '| sort +1 –22' donne d'excellents résultats).

La séquence correspondant au sondage du port 80 sur le système pc0xx est présentée pour information ci-dessous :

```
#/usr/sbin/tcpdump -i eth0 "host 10.A.B.14"
> vts-tests.apogee-com.fr.16414  > pc0xx.apogee-com.fr.http:
  S 4142284908:4142284908(0)                win 4096
  (DF) (ttl 255, id 255)
< pc0xx.apogee-com.fr.http       > vts-tests.apogee-com.fr.16414:
  S 15963703:15963703(0)     ack 4142284909  win 8576 <mss 1460>
  (DF) (ttl 128, id 6934)
> vts-tests.apogee-com.fr.16414  > pc0xx.apogee-com.fr.http:
  R 4142284909:4142284909(0)                win    0
  (DF) (ttl 255, id 0)
```

SYN initial
Empreinte **4142284908**

SYNC,ACK en réponse
Empreinte **4142284908** + 1

RESET

L'utilitaire '**scanrand**' dispose d'options permettant de répartir le travail sur différents systèmes chargés, l'un

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

d'entre eux assurant le rôle de collecteur des résultats. A cette fin, l'adresse IP de ce dernier est inscrite en tant que destination dans les paquets émis par les différents systèmes. De nombreuses évolutions sont annoncées par l'auteur qui devrait faire de cet outil un excellent complément à '**nmap**'.

- **phentropy**

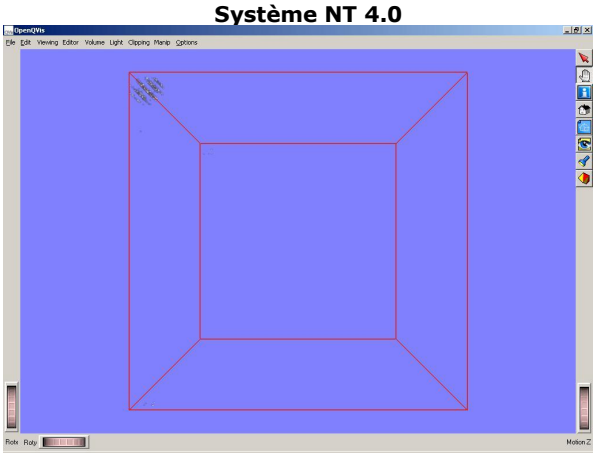
Cet utilitaire est un pré-processeur permettant de traiter un fichier contenant une liste de numéros de séquence **TCP** générés par le système dont on veut caractériser le caractère aléatoire. Le traitement effectué reprend les principes exposés par **Michel Zalewski** dans son article '**Phase Space Analysis of TCP/IP Sequence Numbers**' publié en 2001. Les résultats des calculs sont sauvegardés dans un format permettant leur visualisation en 3 dimensions par l'outil libre '**OpenQVis**' fonctionnant en environnement **UNIX**, **Mac** et **Windows**.

```
#./phentropy -a -v
# ls -l logfile*
-rw-rw-r--    1 bvel     adm       303104 Dec  5 15:55 logfile
-rw-rw-r--    1 bvel     adm          221 Dec  5 15:56 logfile.dat
-rw-rw-r--    1 bvel     adm     16777216 Dec  5 15:56 logfile.raw
```

Fichier source
Fichiers pour visualisation sous OpenQVis

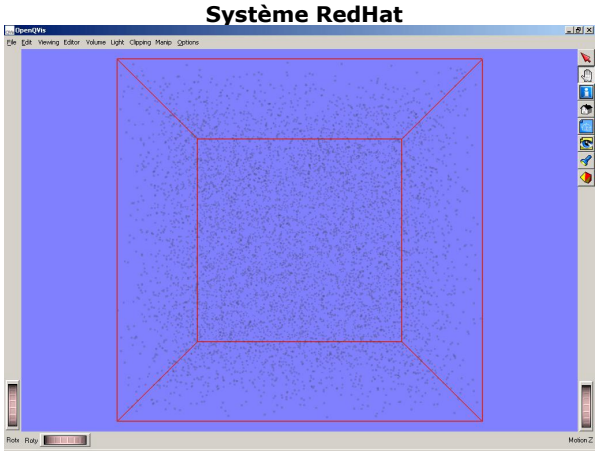
Un exemple de résultats graphiques est proposé ci-dessous. Ceux-ci ont été générés à partir de la collecte des numéros de séquence TCO produit par la pile TCP/IP d'un système NT 4.0 n'ayant fait l'objet d'aucune mise à jour et d'un système RedHat récent.

Système NT 4.0



Concentration des données qui prennent la forme d'une structure régulière en haut à gauche : les numéros de séquence sont prédictibles.

Système RedHat



Répartition spatiale des données ne mettant en évidence aucun schéma a priori structuré : la prédiction sera difficile.

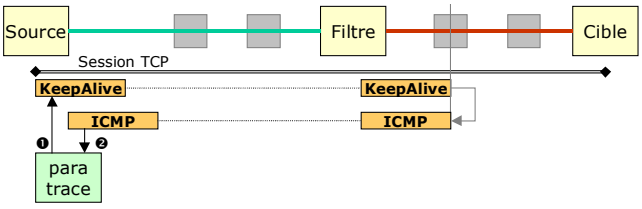
Les numéros de séquence ont ici été acquis à l'aide de l'utilitaire '**gather**' qui utilise les outils '**netcat**' et '**tcpdump**' pour générer du trafic vers une cible identifiée et journaliser les numéro de séquence générée par celle-ci. '**gather**' est livré dans le paquetage '**vseq**' proposé par **M. Zalewski** sur le site de la société **BindView**. La mise en œuvre de l'application '**OpenQvis**' nécessite une machine très performante dotée d'une carte vidéo comportant un accélérateur OpenGL matériel et d'au moins 384Mo de mémoire vive

- **paratrace**

Cet utilitaire permet d'identifier la route suivie par une connexion '**TCP**' sans utiliser aucune des méthodes peu discrètes habituellement employées car portant sur l'utilisation explicite de paquets de sondages **ICMP** ou **UDP**.

Le procédé retenu – astucieusement nommé '**Parasitic** trace route' par l'auteur - consiste à tirer parti d'une session **TCP** existante officiellement établie à travers un dispositif de filtrage de paquets pour transmettre sur cette même session une série de paquets **TCP** dits de '**KeepAlive**'.

Ces paquets sont caractérisés par le positionnement des flags '**ACK**' et '**PUSH**' et l'utilisation d'un numéro de séquence explicitement positionné en dehors de la fenêtre d'acquittement afin de forcer une réponse – un acquittement – de la part de la cible ou une réponse **ICMP** '**Time Exceeded**' de la part d'un quelconque équipement de routage situé entre l'émetteur et la cible.



L'analyse des réponses 'Time Exceeded' permet de reconstituer le parcours suivi, sous réserve que ces paquets ne soient pas filtrés ! La mise en œuvre de ce procédé quelque peu particulier consiste à activer l'utilitaire '**paratrace**' en précisant le système ou le réseau cible, puis à établir par ailleurs une session 'légale' vers celui-ci.

Un exemple de fonctionnement est proposé ci-dessous. La politique de filtrage mise en œuvre interdit le bon fonctionnement de l'utilitaire ultra-classique '**trace-route**' :

```
# traceroute ftp.ciac.org
traceroute to ciac.org (198.128.39.4), 30 hops max, 38 byte packets
1  * * *
2  * * *
3  * * *
4  * * *
```

Cette même politique qui ne filtre pas les réponses ICMP en provenance des réseaux externes autorise le parfait

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

fonctionnement de l'outil '**paratrace**' :

```
# paratrace ftp.ciac.org
  Waiting to detect attachable TCP connection to host/net: ftp.ciac.org
  198.128.39.4:21/32 1-22
  001 =      192.A.C.3|21      [01]   2.062s (     192.A.B.2 -> 198.128.39.4    )
  002 =     62.23.184.29|21    [02]   2.069s (     192.A.B.2 -> 198.128.39.4    )
  003 =     62.23.184.13|21    [03]   2.071s (     192.A.B.2 -> 198.128.39.4    )
  004 =    195.68.60.253|21    [04]   2.074s (     192.A.B.2 -> 198.128.39.4    )
  005 =    195.68.85.188|21    [05]   2.075s (     192.A.B.2 -> 198.128.39.4    )
  006 =     212.74.67.33|21    [06]   2.075s (     192.A.B.2 -> 198.128.39.4    )
  007 =    212.74.74.169|21    [10]   2.172s (     192.A.B.2 -> 198.128.39.4    )
  008 =      4.25.133.37|21    [10]   2.173s (     192.A.B.2 -> 198.128.39.4    )
  009 =         4.0.7.14|21    [10]   2.174s (     192.A.B.2 -> 198.128.39.4    )
  010 =      4.24.10.177|21    [10]   2.177s (     192.A.B.2 -> 198.128.39.4    )
  011 =       4.24.10.90|21    [11]   2.177s (     192.A.B.2 -> 198.128.39.4    )
  012 =      4.24.10.185|21    [13]   2.180s (     192.A.B.2 -> 198.128.39.4    )
  013 =       4.24.10.29|21    [14]   2.181s (     192.A.B.2 -> 198.128.39.4    )
  014 =       4.24.4.110|21    [14]   2.182s (     192.A.B.2 -> 198.128.39.4    )
  015 =      4.24.144.70|21    [16]   2.183s (     192.A.B.2 -> 198.128.39.4    )
  016 =    134.55.209.77|21    [17]   2.184s (     192.A.B.2 -> 198.128.39.4    )
  017 =    134.55.209.17|21    [18]   2.212s (     192.A.B.2 -> 198.128.39.4    )
  018 =   134.55.205.122|21    [15]   2.254s (     192.A.B.2 -> 198.128.39.4    )
  019 =   134.55.208.238|21    [15]   2.256s (     192.A.B.2 -> 198.128.39.4    )
  020 =     192.188.35.2|21    [16]   2.257s (     192.A.B.2 -> 198.128.39.4    )
  021 =    198.128.38.10|21    [17]   2.258s (     192.A.B.2 -> 198.128.39.4    )
  UP:      198.128.39.4:21     [18]   3.380s
```

On remarquera que cette méthode nous dévoile un système normalement masqué par la présence d'un dispositif de filtrage en amont de la cible. En effet, un 'traceroute' effectué à partir d'un compte autorisé ne révèle pas le système d'adresse 198.128.38.10.

```
# traceroute ftp.ciac.org
  Tracing route to ciac.org [198.128.39.4]
  over a maximum of 30 hops:
   1   <10 ms    10 ms   <10 ms  192.A.B.3
   2   <10 ms    10 ms   <10 ms  62.23.184.29
   3   <10 ms    10 ms   <10 ms  62.23.184.13
   4    10 ms    10 ms    10 ms  wan253.60.68.195.rev-watt.coltfrance.com [195.68.60.253]
   5   <10 ms    10 ms    10 ms  gi1-0.bbr2-wat.fr.colt.net [195.68.85.188]
   6   <10 ms   <10 ms    10 ms  pos1-0-obelix.par.router.colt.net [212.74.67.33]
   7   100 ms   111 ms   100 ms  pos1-1-kyle.nyc.router.colt.net [212.74.74.169]
   8   100 ms   110 ms   121 ms  so-4-1-1.nycmny1-hcr3.bbnplanet.net [4.25.133.37]
   9   100 ms   100 ms   100 ms  p10-0.nycmny1-nbr2.bbnplanet.net [4.0.7.14]
  10   100 ms   120 ms   110 ms  p9-0.phlapa1-br1.bbnplanet.net [4.24.10.177]
  11   110 ms   121 ms   120 ms  p15-0.phlapa1-br2.bbnplanet.net [4.24.10.90]
  12   110 ms   100 ms   121 ms  so-0-0-0.washdc3-nbr2.bbnplanet.net [4.24.10.185]
  13   110 ms   100 ms   130 ms  so-7-0-0.washdc3-nbr1.bbnplanet.net [4.24.10.29]
  14   120 ms   110 ms   130 ms  p1-0.washdc3-cr5.bbnplanet.net [4.24.4.110]
  15   110 ms   121 ms   120 ms  mae-east-atm-gtei.es.net [4.24.144.70]
  16   110 ms   110 ms   131 ms  dccr1-ge0-dcpr1.es.net [134.55.209.77]
  17   130 ms   140 ms   130 ms  orn-dchub.es.net [134.55.209.17]
  18   180 ms   200 ms   170 ms  snv-s-orn.es.net [134.55.205.122]
  19   180 ms   190 ms   201 ms  llnl-oc3-snv.es.net [134.55.208.238]
  20   190 ms   200 ms   191 ms  llnl-foutside.llnl.gov [192.188.35.2]
  21     *        *        *     Request timed out.
  22     *        *        *     Request timed out.
  23     *        *
```

- **lc**

L'utilitaire '**lc**' (LinkCat) est le pendant de '**nc**' (NetCat) mais fonctionnant au niveau 'liaison' (trame ethernet) et non au niveau 'réseau' (paquet IP) comme cela est le cas avec '**nc**'. Tout comme avec son homologue, les fonctions offertes permettent d'absorber un trafic ethernet spécifique, voire d'usurper ou de rediriger celui-ci avec les limitations inhérentes au niveau d'intervention : la couche Ethernet.

L'option '**-m**' est particulièrement intéressante car elle permet de transmettre des données acquises sur le flux d'entrée du programme (stdin) ou contenues dans un fichier sous la forme de trames '**ethernet**'. Il est ainsi aisé de générer ou manipuler un quelconque trafic au niveau Ethernet.
Une utilisation basique consistera à acquérir le trafic 'ethernet' du lien sur lequel est attaché le poste, le trafic 'icmp' dans l'exemple suivant:

```
# lc -l eth0 -p imcp
  00 10 a4 14 4f 51 00 a0 c9 1d da fb 08 00 45 10 00 28 60 86 40 00 40 06 a9 9c \
  0a 21 0e 2b 0a 21 0e 31 00 16 09 ce ca 97 ef 19 d5 e5 3a 28 50 10 16 d0 94 c3 \
  00 00
  00 10 a4 14 4f 51 00 a0 c9 1d da fb 08 00 45 10 00 3c 60 87 40 00 40 06 a9 87 \
  0a 21 0e 2b 0a 21 0e 31 00 16 09 ce ca 97 ef 19 d5 e5 3a 28 50 18 16 d0 d1 bd \
  00 00 00 00 00 0b 69 3a 43 b3 2a 69 32 bd bc 01 47 d5 00 56 b4 9d
```


© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

```
  00 10 a4 14 4f 51 00 a0 c9 1d da fb 08 00 45 10 00 74 60 88 40 00 40 06 a9 4e \
  0a 21 0e 2b 0a 21 0e 31 00 16 09 ce ca 97 ef 2d d5 e5 3a 28 50 18 16 d0 d3 0d \
  00 00 00 00 00 44 44 ac 18 4a a6 8d 60 a7 f7 a1 cc db c6 ec 06 bd a5 45 f9 67 \
  d8 11 bd 26 51 e4 03 10 eb d5 8b d4 94 47 d8 25 e8 c1 b5 d3 fb 93 c7 c5 d1 9b \
  90 b4 43 7d 2d 9f db 6a d8 a4 c1 4d 96 e5 70 d0 d8 0c 04 13 d5 7c 9f 80 5a 37
  00 a0 c9 1d da fb 00 10 a4 14 4f 51 08 00 45 00 00 28 57 e7 40 00 80 06 72 4b \
  0a 21 0e 31 0a 21 0e 2b 09 ce 00 16 d5 e5 3a 28 ca 97 ef 79 50 10 f9 ac b1 86 \
  00 00 00 00 00 0c 8a 55
```

Il est aussi possible de transférer tout le trafic '**ethernet**' reçu sur une interface vers une seconde interface:

```
# lc -l eth0 | lc -m eth1
```

Les règles de filtrage usuelles en environnement 'tcpdump' (ou de tout autre produit utilisant la librairie d'interface paquet dite 'libpcap') sont ici applicables.

On notera que les options '**-M**', '**-M**' et '**-S**' permettent d'insérer, de vérifier ou d'éliminer une signature positionnée après dans la zone résiduelle (ou '**trailer**') d'une trame 'ethernet' aucun sans impact sur l'intégrité et la validité des données transportées. A titre d'exemple, un paquet ARP normalement constitué - longueur utile de 42 octets sur une longueur transmise de 60 octets - est structuré comme suit:

Paquet ARP normal

```
Frame 54 (60 on wire, 60 captured)
Arrival Time: Dec  9, 2002 14:07:53.308875000
    Time delta from previous packet: 0.000446000 seconds
    Time relative to first packet: 4.103221000 seconds
    Frame Number: 54
    Packet Length: 60 bytes
    Capture Length: 60 bytes
Ethernet II
    Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source: 00:01:02:17:a4:b1 (00:01:02:17:a4:b1)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000...
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6

Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:01:02:17:a4:b1 (00:01:02:17:a4:b1)
    Sender IP address: 11.12.13.14 (11.12.13.14)
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 11.12.13.15 (11.12.13.15)
0000  ff ff ff ff ff ff 00 01 02 17 a4 b1 08 06 00 01   ................
0010  08 00 06 04 00 01 00 01 02 17 a4 b1 0b 0c 0d 0e   ..............!.U
0020  00 00 00 00 00 00 0b 0c 0d 0f 00 00 00 00 00 00   .......!........
0030  00 00 00 00 00 00 00 00 00 00 00 00
```

Ce même paquet peut être ré-émis après capture en intégrant une signature au moyen de la commande suivante:

```
# lc -m eth1 -r capture.txt -M TestKey
```

La structure du paquet modifié devient la suivante:

Paquet ARP contenant une signature

```
Frame 43 (80 on wire, 80 captured)
Arrival Time: Dec  9, 2002 14:17:37.435213000
    Time delta from previous packet: 0.000499000 seconds
    Time relative to first packet: 3.449064000 seconds
    Frame Number: 43
    Packet Length: 80 bytes
    Capture Length: 80 bytes
Ethernet II
    Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source: 00:01:02:17:a4:b0 (00:01:02:17:a4:b0)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000...
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:01:02:17:a4:b0 (00:01:02:17:a4:b0)
    Sender IP address: 11.33.14.85 (11.33.14.85)
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 11.33.14.210 (11.33.14.210)
```


© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

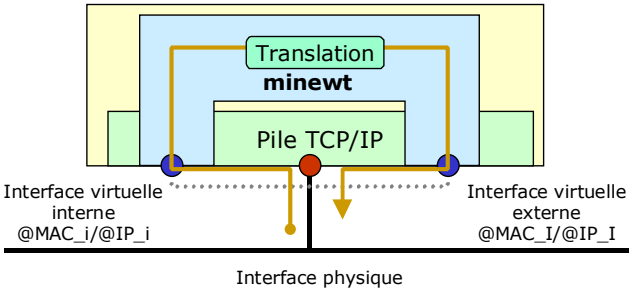
```
0000   ff ff ff ff ff ff 00 01 02 17 a4 b0 08 06 00 01   ................
0010   08 00 06 04 00 01 00 01 02 17 a4 b0 0b 0c 0d 0e   ..............!.U
0020   00 00 00 00 00 00 0b 0c 0d 0f 00 00 00 00 00 00   .......!........
0030   00 00 00 00 00 00 00 00 00 00 00 00 c6 05 8a      ................
0040   f3 c5 70 f6 a5 9c 1d 05 63 04 59 a4 32 b2 26 ba   ..p.....c.Y.2.&.
```

Ce procédé peut permettre l'établissement d'un canal de communication masqué (ou 'covert channel' dans le jargon) entre deux systèmes d'un même réseau physique.

- **Minewt**

Cet utilitaire - le plus complexe du paquetage - a été conçu comme démonstrateur des concepts de manipulation présentés par l'auteur. Il offre la possibilité de gérer les connexions réseaux comme le ferait un équipement de routage en s'exécutant en environnement utilisateur et donc sans avoir à être installé en tant que gestionnaire de périphériques dans le noyau LINUX.

L'utilitaire '**minewt**' se comporte comme une passerelle IP permettant d'assurer la classique fonction de translation d'adresse IP ou 'NAT' mais aussi une fonctionnalité dénommée 'MAT' - ou MAC Address translation - permettant de manipuler dynamiquement la table ARP (table maintenant l'association [adresse MAC (niveau 2) / adresse IP (niveau3)].



Les possibilités de cet utilitaire sont trop nombreuses pour être toutes citées et faire l'objet de tests exhaustifs, d'autant que la majorité des utilisations conduira à mettre en péril l'intégrité du réseau.

Ainsi, la simple initialisation de '**minewt**' fera apparaître sur le réseau une nouvelle adresse **IP** derrière laquelle pourront se cacher une multitude de systèmes si la fonction de translation d'adresse MAC est activée.

L'auteur mentionne l'utilisation de cet outil dans le contexte de ce qu'il appelle '**Guerrila Multicast**' consistant à associer une adresse IP du réseau avec une adresse MAC réservée dite de multicast (de la forme 01:00:5E:xx:xx:xx). Dès lors, toute réponse transmise à cette adresse IP sera immédiatement rediffusée à l'ensemble des équipements du sous-réseaux, les équipements de commutation assurant automatiquement cette fonction dans le cas d'une infrastructure commutée.

On notera pour finir que les deux adresses MAC suivantes sont utilisées par défaut sur les deux interfaces virtuelles créées par '**minewt**': interface interne '**00:AB:BA:5A:AB:BA**', interface externe '**00:01:56:78:9a:bc**'. L'apparition de l'une de ces 2 adresses MAC sur un segment peut conduire à supposer qu'une passerelle '**minewt**' est active.

- **Complément d'information**

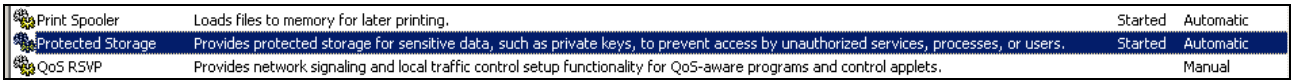
http://www.doxpara.com
http://www.doxpara.com/read.php/docs/pk_english.html
http://razor.bindview.com/publish/papers/tcpseq.html
http://razor.bindview.com/publish/papers/tcpseq/vseq.tgz
http://sourceforge.net/projects/openqvis

TECHNIQUES

WINDOWS PROTECTED STORAGE

- **Description**

Le lecteur habitué de l'environnement Windows aura probablement remarqué l'existence d'un service dénommé '**Protected Storage**' (ou '**Emplacement protégé**' dans la version Française). Apparu sous Windows NT 4.0, ce service n'a jamais été précisément documenté à l'exception peut être de la description assez précise apparue dans le gestionnaire de service livré avec Windows 2000.


Print Spooler
Loads files to memory for later printing.
Started
Automatic
Protected Storage
Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.
Started
Automatic
QoS RSVP
Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.
Manual

La colonne 'description' nous annonce en effet:

Protected Storage	*Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes or user*
Emplacement Protégé	*Fournit un stockage protégé pour les données sensibles, telles que les clefs privées, afin d'empêcher l'accès par des services, des processus ou des utilisateurs non autorisés*

Ainsi, ce service assure la sauvegarde d'informations sensibles dans un contexte accessible aux utilisateurs mobiles, celles-ci étant archivées en tant qu'éléments du profil utilisateur. Sont gérés par ce service : les clefs privées de l'utilisateur, les données saisies dans les formulaires WEB, les mots de passe requis par les ressources WEB protégées, les authentifiants d'accès aux comptes de messagerie Outlook …

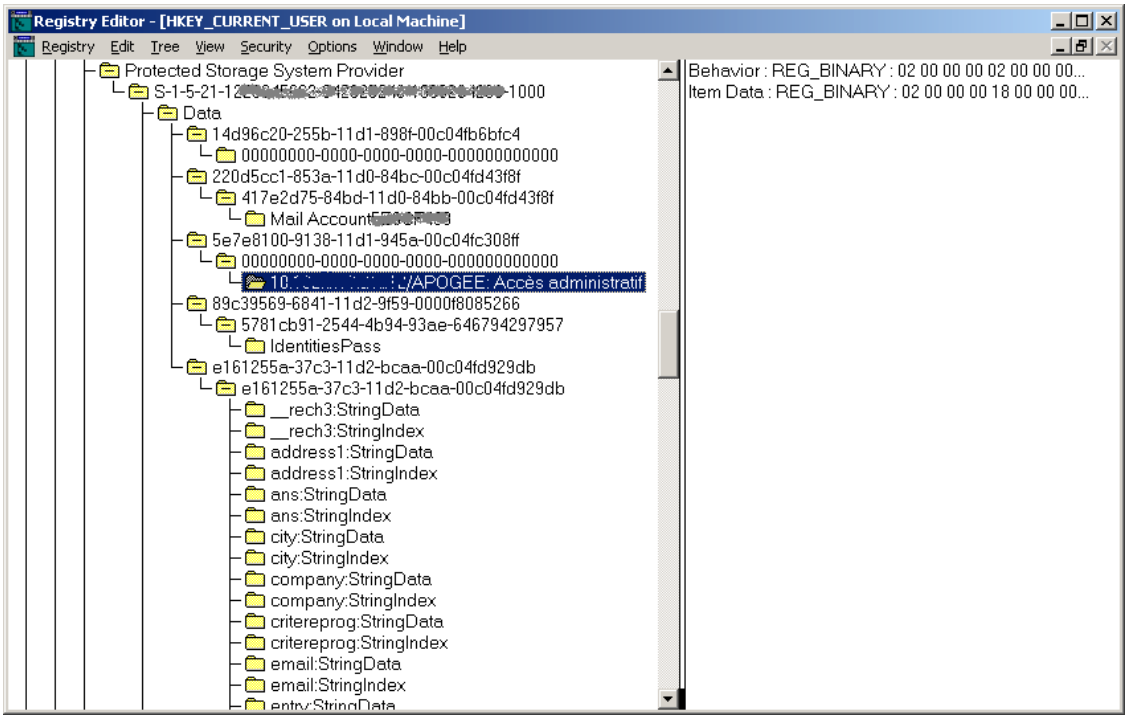
Aucune documentation concernant l'interface d'accès à ces données annoncées sauvegardées chiffrées n'est officiellement disponible à l'exception de la référence de la clef d'identification dans la base de registre:

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

La visualisation de cette clef à l'aide de l'outil '**RegEdt32**' met en évidence la présence d'une entrée contenant

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

l'identifiant de l'utilisateur courant – dit **SSID** – sans qu'il soit possible de visualiser les éléments associés à cette entrée. L'ajout d'une autorisation de lecture sur cette entrée dévoile la structure de sauvegarde utilisée par le service:



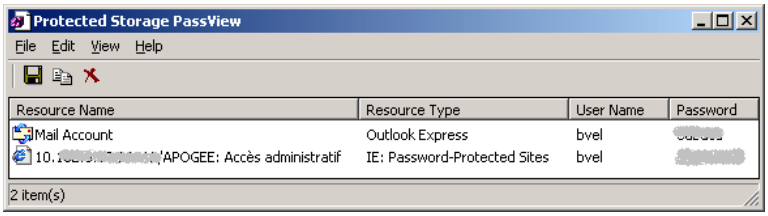
Un rapide parcours des attributs '**Behavior**' et '**Item Data**' liés aux clefs a priori sensibles ne permet pas de mettre en évidence un quelconque contenu en clair ce qui semble confirmer la présence d'un protection contre la perte de confidentialité.

Notre étude de ce service aurait pu s'arrêter ici si certains développeurs n'avaient mis en évidence l'existence d'une interface programmatique offrant toutes les fonctions d'accès requises, interface exposée sous la forme d'un objet **DCOM** par la librairie dynamique '**pstorec.dll**'. Actuellement, les seules fonctions ayant fait l'objet d'une rétro-analyse sont celles permettant d'énumérer les éléments gérés par le service. Il n'en fallait pas plus pour voire fleurir nombre de logiciels permettant de visualiser les données gérées en clair, et pour certains outils, de modifier celles-ci.

Trois outils ont ainsi attirés notre attention:

Passview

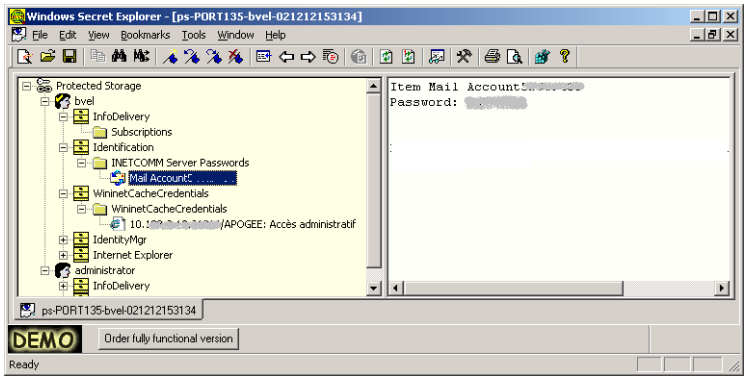
Utilitaire gratuit, '**Passview**' offre une interface graphique permettant de révéler les identifiants et mots de passe de l'utilisateur courant dans un format directement exploitable. En effet, chaque champ est présenté décodé en indiquant la ressource ayant sauvegardé celui-ci.



L'utilitaire '**Passview**' qui prend la forme d'un exécutable totalement autonome de 70Ko, permet de visualiser et de détruire les identifiants et mots de passe des comptes Outlook Express, les identifiants et mots de passe protégeant l'accès aux ressources WEB accédées via Internet Explorer et enfin, les mots de passe mémorisés à la suite de leur saisie dans un formulaire WEB.

Windows Secret Explorer

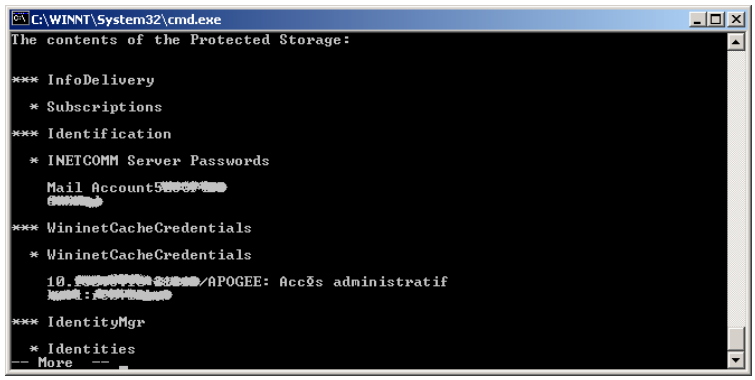
Utilitaire commercial - une version de démonstration est librement accessible - '**WSE**' offre la possibilité de manipuler la totalité du contenu de la zone de sauvegarde protégée du poste local mais aussi de n'importe quel poste distant pour quiconque dispose des privilèges 'administrateur'.
Cet utilitaire est vendu en tant qu'outil d'investigation – forensic – et de récupération – recovery – des mots de passe.



pStoreView

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

Contrairement aux autres produits, '**pStoreView**' fonctionne en mode texte et n'offre aucune possibilité de modifier ou d'éditer les données.
Le code source de cet utilitaire n'est pas disponible ce qui en limite fortement l'intérêt.
On notera cependant que l'auteur - **Arne VidStrom** - propose quelques 39 outils d'analyse et d'attaque sur son site '**NTSecurity.nu**'.
Parmi ceux-ci quatre outils pourront plus particulièrement être utilisés par un investigateur:



ListModule	**ListModule** permet de lister les modules – **EXE** et **DLL** - chargés en mémoire par un processus WIN32.
LNS	**LNS**, sigle de **L**ist **N**TFS **S**treams, permet de lister les streams auxiliaires d'un fichier. Ce mécanisme a fait l'objet d'un article dans le rapport N°41 Décembre 2001.
PEriscope	**PEriscope** permet d'inspecter la structure et le contenu d'un fichier exécutable WIN32 au format PE. Cet utilitaire offre toutefois moins d'informations que l'outil bien connu '**DumpBin**'.
PMDUMP	**PMDump** permet d'obtenir une copie de la mémoire allouée à certains processus sans avoir à arrêter ceux-ci. Le fichier ainsi obtenu pourra ensuite être analysé.

▪**Complément d'information**

http://www.codeproject.com/w2k/pseenuma.asp?print=true
http://ntsecurity.nu/toolbox/pstoreview/
http://lastbit.com/wse/default.asp
http://nirsoft.multiservers.com/utils/pspv.zip

OPENSSL / SLAPPER 6 MOIS APRES

▪**Description**

Le mois de juillet 2002 devait voir la publication de l'une des vulnérabilités les plus critiques jamais encore dévoilée car portant sur l'un des **paquetages** de sécurité les plus en vogue, **OpenSSL**.

L'avis de sécurité publié le 30 juillet dans la liste de diffusion Bugtraq annonçait la découverte de 5 vulnérabilités majeures dont trois pouvaient être exploitées dans l'optique de faire exécuter un quelconque code sur tout serveur offrant une session protégée par l'implémentation **OpenSSL** du protocole **SSL** mais aussi sur le client ayant établi celle-ci :

1- Le message **SSLv2** '**CLIENT-MASTER-KEY**' est incorrectement géré. Un client peut alors transmettre une version spécialement formatée de ce message pour provoquer un débordement de buffer sur le serveur et exécuter le code de son choix dans le contexte de l'application utilisant **SSL**. Ce message est transmis durant la phase de négociation du protocole **SSL** donc préalablement à toute identification du client.

2- L'envoi d'un identifiant de session **SSLv3** d'une taille supérieure à celle spécifiée et gérée par le client conduit à un débordement de buffer autorisant l'envoi et la transmission par le serveur d'un code qui sera exécuté sur le client. Ici encore, la phase de transmission de cet identifiant – **SessionID** – intervient durant la phase initiale de négociation de la session SSL.

3- La fourniture d'une clef maître **SSLv3** d'une taille supérieure à celle spécifiée et gérée par le serveur conduit à un débordement de buffer autorisant la transmission par le client d'un code qui sera exécuté sur le serveur. Ce problème n'affecte que les versions préliminaires d'OpenSSL 0.9.7.

4- Plusieurs zones tampons utilisées pour assurer la conversion de nombres entiers sous la forme de chaînes ASCII ont une taille insuffisante pour assurer cette opération sur les plates-formes 64 bits.

5- L'analyseur syntaxique **ASN1** peut être conduit en erreur en lui fournissant différents encodages invalides.

L'extrême criticité de ces vulnérabilités – en particulier les 2 premières - a conduit la majorité des éditeurs à réagir dans les 24 heures ayant suivies la diffusion de l'alerte par la publication de correctifs palliatifs dans l'attente d'une nouvelle version immune de la plate-forme **OpenSSL**. Le 9 août 2002 était enfin mise à disposition la version **OpenSSL** 0.9.6g corrigeant non seulement les vulnérabilités publiquement annoncées mais aussi divers problèmes n'ayant jamais fait l'objet d'aucune communication.

Rappelons que le paquetage **OpenSSL** intègre deux constituants complémentaires :

- la libraire '**libssl**' regroupant l'ensemble des fonctionnalités cryptographiques et protocolaires nécessaires à l'établissement et à la gestion d'une session **SSL**,
- l'utilitaire '**openssl**' offrant une interface permettant la génération et la validation des éléments cryptographiques utilisés lors de l'établissement d'une session **SSL**, ou plus largement, toutes les opérations de gestion de certificats X509.

Les problèmes découverts dans ce paquetage résidaient tous dans les fonctions de gestion du protocole **SSL**. En conséquence, n'étaient vulnérables que les applications utilisant ce paquetage, c'est à dire plus précisément la librairie '**libssl**', pour ses fonctionnalités de gestion du protocole **SSL** et non pour les seules fonctions cryptographiques.

Cette dualité dans l'utilisation du paquetage '**OpenSSL**' fût à l'origine d'une certaine confusion dans les alertes émises

© APOGEE Communications - Tous droits réservés
Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE

les premiers jours où, dans un soucis d'application du principe de précaution, plusieurs applications utilisant '**OpenSSL**' en tant que librairie cryptographique ont été annoncées vulnérables. Avec le recul dont nous disposons désormais, force est de constater que la majorité des attaques ont porté sur les serveurs WEB Apache fonctionnant en environnement LINUX ou BSD.

Pour compléter cette brève synthèse des conditions ayant conduit à l'apparition des différentes versions du ver '**Slapper**', nous devons rappeler que quelques mois avant la publication de l'alerte par l'équipe de développement d'**OpenSSL**, des rumeurs persistantes faisaient état de l'existence d'un code d'exploitation privé tirant parti d'une vulnérabilité dans **OpenSSL**, rumeurs n'ayant jamais été confirmées par la publication du dit code, du moins jusqu'à la diffusion du code '**openssl-too-open.c**' dans la liste '**FullDisclosure**', le 17 Septembre 2002 par **Solar Eclipse**.

A cette date, un ver exploitant la même vulnérabilité circulait déjà depuis 5 jours sur l'Internet dont une copie était capturée par le plus grand des hasards le 13 septembre. Analysé en détail dans les jours suivant sa découverte et baptisé '**Modap**' puis '**Slapper.A**', ce ver devait faire l'objet de très nombreuses évolutions en quelques semaines. Pour mémoire, la version '**B**' de ce ver a fait l'objet du défi N°25 lancé le mois dernier par le projet '**HoneyNet**' (Rapport N°52 – Novembre 2002).

Les conditions d'évolution assez particulières de cette vulnérabilité aisément détectable à distance et pour laquelle une vaste campagne d'information a très rapidement été engagée par les éditeurs et organismes de sécurité en font un objet d'étude idéal pour qui souhaite déterminer au jour le jour le comportement des administrateurs et des exploitants de systèmes vulnérables.

Eric Rescorla, un consultant de la société '**RTFM Inc**' a ainsi décidé de suivre sur plus de 3 mois l'évolution du niveau de mise à jour de quelques 890 serveurs WEB Apache initialement découverts vulnérables à la vulnérabilité SSL v2 dite '**CLIENT-MASTER-KEY**'.

Les résultats de cette étude ont été publiés début décembre dans un rapport intitulé '**Security Holes... Who Cares**' dont les conclusions sont pour le moins alarmantes: deux semaines après l'annonce des vulnérabilités touchant **OpenSSL**, seuls 23% des serveurs initialement vulnérables avaient fait l'objet d'une mise à jour. Il aura fallu attendre l'apparition du ver '**Slapper**' pour que cette proportion passe à 40%.

L'auteur de l'étude considère qu'il s'agit ici du résultat de l'attitude '**Wait & See**' trop souvent rencontrée dans le contexte des problèmes de sécurité. L'annonce de l'existence d'un code d'exploitation, un ver en l'occurrence, aura participé plus que tout autre élément d'information à la prise de conscience de l'urgence de la mise à niveau des systèmes.

Nous recommandons la lecture de ce rapport d'étude remarquable à plus d'un point de vue : analyse statistique rigoureuse et largement documentée, résultats démontrant non seulement l'importance de la diffusion d'un code d'exploitation à large échelle sur le déclenchement des mises à jour mais aussi l'impact des mécanismes et procédés de diffusion des correctifs sur le niveau de sécurité final.

Ainsi, et à ce propos, la diffusion à quelques semaines d'intervalle d'une version 'palliative' (OpenSSL 0.9.6e) puis d'une dernière version totalement stabilisée (OpenSSL 0.9.6g) à conduit à l'installation massive de la première hélas non suivie d'une mise à jour vers la dernière version disponible. On notera par ailleurs, l'anecdote concernant une dizaine d'infrastructures cibles utilisant un mécanisme de partage de charge pour lesquels tous les serveurs WEB n'avaient pas été mis à jour !

L'histoire étant un éternel recommencement, le 16 décembre, la société **Rapid7**, l'éditeur de '**NeXpose**', un analyseur de vulnérabilité commercial, annonce avoir mis en évidence plusieurs vulnérabilités exploitables dans une dizaine d'implémentations du protocole **SSH** (Avis d'alerte Rapid7 **R7-0009** et **CERT CA-2002-36**). Localisées dans la phase initiale d'annonce et d'échange de clefs, ces vulnérabilités peuvent être exploitées pour provoquer un débordement de buffer dans le code du serveur ou du client **SSH** et ainsi en prendre le contrôle. Cette alerte prend toute son importance à la lueur des résultats de l'étude '**Security Holes... Who Cares**' …

- **Complément d'information**

http://www.rtfm.com/upgrade.pdf

http://www.rtfm.com/pubs.html

http://www.rapid7.com/perl/DownloadRequest.pl?PackageChoice=666

http://online.securityfocus.com/archive/1/285022

© APOGEE Communications - Tous droits réservés Diffusion restreinte aux clients abonnés aux services VTS-RAPPORT et VTS-ENTREPRISE